IBM Tivoli Access Manager for e-business

BEA WebLogic Server 통합 안내서

버전 5.1

SA30-2210-00

IBM Tivoli Access Manager for e-business

BEA WebLogic Server 통합 안내서

버전 5.1

SA30-2210-00

주!

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 71 페이지의 부록 C『주의사항』을 읽으십시오

초판(2003년 11월)

이 개정판은 새 개정판에 별도로 명시하지 않는 한, IBM Tivoli Access Manager(제품 번호 5724-C08)의 버전 5, 릴리스 1, 수정사항 0 및 모든 후속 릴리스와 수정사항에 적용됩니다.

© Copyright International Business Machines Corporation 2003. All rights reserved.

목차

서문. vii
이 책의 사용자 vii
이 책의 내용 viii
관련 서적. viii
릴리스 정보 viii
기본 정보 ix
웹 보안 정보 ix
개발자 참조서 x
기술 보충 설명서. xi
관련 서적 xi
온라인 서적 액세스. xv
특수 액세스 기능 xv
소프트웨어 지원 문의 xv
이 책에 사용된 규칙 xvi
글자체 규칙 xvi
운영체제에 따른 변수 및 경로 xvi

제 1 장 소개 및 개요 1
Tivoli Access Manager 보안 모델. 1
Tivoli Access Manager 및 WebLogic 서버 통합. 2
Tivoli Access Manager Security Service Provider Interface 구성요소 3
Policy 및 역할 배치. 5
자원 및 역할 5
Tivoli Access Manager 인증 사용. 6
로깅 및 감사 8
신뢰성, 가용성, 크기 조정 가능성 8

제 2 장 설치 지시사항 11
지원되는 플랫폼 11
디스크 및 메모리 요구사항 11
사전 설치 소프트웨어 12
Tivoli Access Manager Policy Server 12
Tivoli Access Manager Authorization Server 12
Tivoli Access Manager WebSEAL 또는 Tivoli Access Manager Plug-in for Web Servers 13
BEA WebLogic Server 13
Tivoli Access Manager Java 런타임 14
설치 마법사를 사용하여 설치 14
install_amwls 옵션. 16
원시 유틸리티를 사용하여 설치 17
AIX에 설치 17
HP-UX에 설치 18
Solaris에 설치 19

© Copyright IBM Corp. 2003

Windows에 설치 20

제 3 장 구성 절차 23
제 1 부: Tivoli Access Manager Java Runtime Environment 구성 23
제 2 부: startWebLogic에 대한 CLASSPATH 설정 25
제 3 부: Tivoli Access Manager for WebLogic 구성 26
Console Extension Web Application을 사용하여 Tivoli Access Manager for WebLogic 구성. 26
명령행에서 Tivoli Access Manager for WebLogic 구성 28
제 4 부: Tivoli Access Manager 범위 구성 29
Console Extension Web Application을 사용하여 Tivoli Access Manager 범위 구성 29
명령행에서 Tivoli Access Manager 범위 구성 30
제 5 부: BEA WebLogic Server 싱글 사인 온 구성 32
WebSEAL 정션을 사용하여 싱글 사인 온 구성 32
Tivoli Access Manager Plug-in for Web Servers를 사용하여 싱글 사인 온 구성 33
제 6 부: 클러스터된 환경을 포함하여 BEA WebLogic Server 다중 서버 환경에서 Tivoli Access Manager for WebLogic 구성 34
제 7 부: 구성 테스트 34

제 4 장 싱글 사인 온 사용 가능 37
Tivoli Access Manager WebSEAL을 사용한 싱글 사인 온 37

제 5 장 관리 태스크 39
Tivoli Access Manager Authorization Server에서 인타이틀먼트 서비스 사용 39
Tivoli Access Manager for WebLogic에서 사용자 및 그룹 관리 40
데모 어플리케이션 사용 41
사용 팁. 43
3회 시도 로그온 policy 44
Tivoli Access Manager 범위 삭제 45
Tivoli Access Manager for WebLogic 구성 해제 46
문제점 해결 팁 46
양식 기반 로그인을 사용하는 싱글 사인 온 실패 46
WebLogic 서버에 메모리 예외가 발생함 47
제한사항 47
알려진 문제점 및 문제해결 방법 48

제 6 장 제거 지시사항 49
Solaris에서 제거. 49
Windows에서 제거. 50
AIX에서 제거 50
HP-UX에서 제거 51

부록 A. 특성 파일 참조 53
amsspi.properties 53
rbpf.properties 55
amwlsjlog.properties 60

부록 B. 명령 빠른 참조 63
AMWLSConfigure -action config 64

AMWLSConfigure -action unconfig 66
AMWLSConfigure -action create_realm 67
AMWLSConfigure -action delete_realm 69

부록 C. 주의사항 71
상표. 73

용어. 75

색인. 83

서문

IBM® Tivoli® Access Manager for BEA® WebLogic Server®(이후로는 Tivoli Access Manager for WebLogic)를 사용하시게 된 것을 환영합니다. 이 제품은 IBM Tivoli Access Manager의 기능을 확장하여 BEA WebLogic Server용으로 작성된 어플리케이션을 지원합니다.

IBM® Tivoli® Access Manager(Tivoli Access Manager)는 IBM Tivoli Access Manager 제품군에서 어플리케이션을 실행하는 데 필요한 기본 소프트웨어입니다. 이 제품은 IBM Tivoli Access Manager 어플리케이션을 통합하여 광범위한 권한 부여 및 관리 솔루션을 제공합니다. 통합 솔루션으로 판매되는 이들 제품은 e-business 어플리케이션을 위한 네트워크 및 어플리케이션 보안 policy를 중앙 집중식으로 관리하는 액세스 제어 관리 솔루션을 제공합니다.

주: IBM Tivoli Access Manager는 이전 Tivoli SecureWay® Policy Director의 새로운 이름입니다. Tivoli SecureWay Policy Director 소프트웨어 및 문서에서 사용한 *관리 서버*를 이제부터 *Policy Server*로 부릅니다.

*IBM Tivoli Access Manager for WebLogic Server 사용자 안내서*에는 BEA WebLogic Server가 있는 IBM Tivoli Access Manager 사용에 대한 설치, 구성 및 관리 지시사항이 나와 있습니다.

이 책의 사용자

이 책은 다음 사용자를 대상으로 합니다.

- 보안 관리자
- 네트워크 시스템 관리자
- IT 설계자

사용자는 다음에 대해 잘 알고 있어야 합니다.

- HTTP, TCP/IP, FTP 및 Telnet과 같은 인터넷 프로토콜
- WebLogic Server 시스템의 배치 및 관리
- 인증 및 권한 부여를 포함한 보안 관리

SSL(Secure Sockets Layer) 통신을 사용하는 경우, SSL 프로토콜, 키 교환(공용 및 개인용), 디지털 특성, 암호화 알고리즘 및 CA(Certificate Authority)에 대해 잘 알고 있어야 합니다.

© Copyright IBM Corp. 2003

이 책의 내용

이 책은 다음과 같이 구성되어 있습니다.

- 제 1 장, “소개 및 개요”

  Tivoli Access Manager for WebLogic이 제공하는 인증 및 권한 서비스의 개요를 소개합니다.

- 제 2 장, “설치 지시사항”

  Tivoli Access Manager for WebLogic을 설치하는 방법에 대해 설명합니다.

- 제 3 장, ”구성 절차”

  Tivoli Access Manager for WebLogic을 구성하는 방법에 대해 설명합니다.

- 제 4 장, “관리 태스크”

  표시 어플리케이션을 사용하는 방법에 대해 설명하고, 사용 팁, 문제점 해결 정보 및 제한사항을 제공합니다.

- 제 5 장, “제거 지시사항”

  Tivoli Access Manager for WebLogic을 제거하는 방법에 대해 설명합니다.

관련 서적

어떤 책이 도움이 되는지 판별하려면 Tivoli Access Manager 라이브러리, 먼저 읽어야 할 책 및 관련 책의 설명을 검토하십시오. 필요한 책을 판별한 후 온라인 서적 액세스에 대한 지시사항을 참조하십시오.

IBM Tivoli Access Manager for e-business 제품 자체에 대한 추가 정보는 다음에서 찾을 수 있습니다.

http://www.ibm.com/software/tivoli/products/access-mgr-e-bus/

Tivoli Access Manager 라이브러리는 다음과 같이 구성되어 있습니다.

- 『릴리스 정보』
- ix 페이지의 『기본 정보』
- ix 페이지의 『웹 보안 정보』
- x 페이지의 『개발자 참조서』
- xi 페이지의 『기술 보충 설명서』

릴리스 정보

- *IBM Tivoli Access Manager for e-business Read This First*(GA30-2205-00)

  Tivoli Access Manager 설치 및 시작하기에 대한 정보를 제공합니다.

- *IBM Tivoli Access Manager for e-business 설치하기 전에*(GA30-2206-00)

소프트웨어 제한사항, 문제 해결 보충 설명 및 문서 갱신사항과 같은 최신 정보를 제공합니다.

기본 정보

- *IBM Tivoli Access Manager 기본 설치 안내서*(SA30-2207-00)

  Web Portal Manager 인터페이스를 포함한 Tivoli Access Manager 기본 소프트웨어의 설치 및 구성 방법에 대해 설명합니다. 이 책은 *IBM Tivoli Access Manager for e-business 웹 보안 설치 안내서*의 서브세트이며, IBM Tivoli Access Manager for Business Integration 및 IBM Tivoli Access Manager for Operating Systems와 같은 기타 Tivoli Access Manager 제품과 함께 사용하기 위한 책입니다.

- *IBM Tivoli Access Manager Base Administration Guide*(SC32-1360-00)

  Tivoli Access Manager 서비스 사용에 대한 개념 및 절차에 대해 설명합니다. **pdadmin** 명령을 사용하여 Web Portal Manager 인터페이스에서 태스크를 수행하는 정보를 제공합니다.

웹 보안 정보

- *IBM Tivoli Access Manager for e-business 웹 보안 설치 안내서*(SA30-2208-00)

  Tivoli Access Manager 기본 소프트웨어 및 웹 보안 구성요소에 대한 설치, 구성 및 제거 지시사항을 제공합니다. 이 책은 *IBM Tivoli Access Manager 기본 설치 안내서*의 수퍼세트입니다.

- *IBM Tivoli Access Manager Upgrade Guide*(SC32-1369-00)

  Tivoli SecureWay Policy Director 버전 3.8 또는 Tivoli Access Manager의 이전 버전을 Tivoli Access Manager 버전 5.1로 업그레이드하는 방법을 설명합니다.

- *IBM Tivoli Access Manager for e-business WebSEAL Administration Guide*(SC32-1359-00)

  WebSEAL을 사용하여 보안 웹 도메인의 자원을 관리하는 작업에 관한 백그라운드 자료, 관리 절차 및 기술 참조 정보를 제공합니다.

- *IBM Tivoli Access Manager for e-business IBM WebSphere Application Server 통합 안내서*(SA30-2209-00)

  Tivoli Access Manager를 IBM WebSphere® Application Server와 통합에 대한 설치, 제거 및 관리 지시사항을 제공합니다.

- *IBM Tivoli Access Manager for e-business IBM WebSphere Edge Server 통합 안내서*(SA30-2211-00)

  Tivoli Access Manager를 IBM WebSphere Edge Server 어플리케이션과 통합에 대한 설치, 제거 및 관리 지시사항을 제공합니다.

- *IBM Tivoli Access Manager for e-business Plug-in for Web Servers Integration Guide*(SC32-1365-00)

웹 서버용 플러그인을 사용하여 웹 도메인 보안을 위한 설치, 관리 절차 및 기술 참조 정보를 제공합니다.

- *IBM Tivoli Access Manager for e-business BEA WebLogic Server 통합 안내서* (SA30-2210-00)

  Tivoli Access Manager를 BEA WebLogic Server와 통합에 대한 설치, 제거 및 관리 지시사항을 제공합니다.

- *IBM Tivoli Access Manager for e-business IBM Tivoli Identity Manager Provisioning Fast Start Guide*(SC32-1364-00)

  Tivoli Access Manager 및 Tivoli Identity Manager 통합에 관련된 태스크의 개요를 제공하고 Provisioning Fast Start 콜렉션의 사용 및 설치 방법을 설명합니다.

개발자 참조서

- *IBM Tivoli Access Manager for e-business Authorization C API Developer Reference*(SC32-1355-00)

  Tivoli Access Manager 권한 부여 C API 및 Tivoli Access Manager 서비스 플러그인 인터페이스를 사용하여 Tivoli Access Manager 보안을 어플리케이션에 추가하는 방법을 설명하는 참조 자료를 제공합니다.

- *IBM Tivoli Access Manager for e-business Authorization Java Classes Developer Reference*(SC32-1350-00)

  권한 부여 API의 Java™ 언어 구현을 사용하여 어플리케이션이 Tivoli Access Manager 보안을 사용하는 방법에 대해 참조 정보를 제공합니다.

- *IBM Tivoli Access Manager for e-business Administration C API Developer Reference*(SC32-1357-00)

  관리 API를 사용하여 어플리케이션이 Tivoli Access Manager 관리 태스크를 수행하는 방법에 대해 참조 정보를 제공합니다. 이 문서에서는 관리 API의 C 구현에 대해 설명합니다.

- *IBM Tivoli Access Manager for e-business Administration Java Classes Developer Reference*(SC32-1356-00)

  권한 부여 API의 Java 언어 구현을 사용하여 어플리케이션이 Tivoli Access Manager 관리 태스크를 사용할 수 있는 작업에 관한 참조 정보를 제공합니다.

- *IBM Tivoli Access Manager for e-business Web Security Developer Reference* (SC32-1358-00)

  CDAS(Cross-Domain Authentication Service), CDMF(Cross-Domain Mapping Framework) 및 Password Strength 모듈에 대한 관리 및 프로그래밍 정보를 제공합니다.

기술 보충 설명서

- *IBM Tivoli Access Manager for e-business Command Reference*(SC32-1354-00)

  Tivoli Access Manager와 함께 제공되는 명령행 유틸리티 및 스크립트에 관한 정보를 제공합니다.

- *IBM Tivoli Access Manager Error Message Reference*(SC32-1353-00)

  Tivoli Access Manager에서 생성되는 메시지의 설명과 권장 조치를 제공합니다.

- *IBM Tivoli Access Manager for e-business Problem Determination Guide*(SC32-1352-00)

  Tivoli Access Manager에 관한 문제점 판별 정보를 제공합니다.

- *IBM Tivoli Access Manager for e-business Performance Tuning Guide*(SC32-1351-00)

  사용자 레지스트리로 정의된 IBM Tivoli Directory Server와 함께 Tivoli Access Manager로 구성되는 환경에 관한 성능 조정 정보를 제공합니다.

관련 서적

이 절에서는 Tivoli Access Manager 라이브러리와 관련된 서적을 나열합니다.

Tivoli Software Library에서는 white papers, datasheets, demonstrations, redbooks 및 announcement letters와 같은 다양한 Tivoli 문서를 제공합니다. 다음 웹 사이트에서 Tivoli Software Library를 사용할 수 있습니다.
http://www.ibm.com/software/tivoli/library/

*Tivoli Software Glossary*에는 Tivoli 소프트웨어에 관련된 기술 용어가 정의되어 있습니다. *Tivoli Software Glossary*는 다음 위치에서 영어로만 볼 수 있습니다. Tivoli Software Library(http://www.ibm.com/software/tivoli/library/)에 있는 **Glossary** 링크를 누르십시오.

IBM Global Security Kit

Tivoli Access Manager는 IBM Global Security Kit(GSKit) 버전 7.0을 통한 데이터 암호화 기능을 제공합니다. GSKit는 특정 플랫폼에 대한 *IBM Tivoli Access Manager Base* CD와 *IBM Tivoli Access Manager Web Security* CD, *IBM Tivoli Access Manager Web Administration Interfaces* CD 및 *IBM Tivoli Access Manager Directory Server* CD에 포함되어 있습니다.

GSKit 패키지는 키 데이터베이스, 공용-개인용 키 쌍 및 인증 요청을 작성하는 데 사용되는 iKeyman 키 관리 유틸리티 **gsk7ikm**을 제공합니다. 다음 서적은 Tivoli Information Center 웹 사이트에 있는 IBM Tivoli Access Manager 제품 문서와 같은 절에서 볼 수 있습니다.

- *IBM Global Security Kit Secure Sockets Layer and iKeyman User's Guide*(SC32-1363-00)

  Tivoli Access Manager 환경에서 SSL 통신이 가능하도록 계획하는 네트워크 또는 시스템 보안 관리자를 위한 정보를 제공합니다.

IBM Tivoli Directory Server

IBM Tivoli Directory Server, 버전 5.2는 사용하는 운영 체제의 *IBM Tivoli Access Manager Directory Server* CD에 포함되어 있습니다 .

주: IBM Tivoli Directory Server는 이전에 다음의 이름으로 릴리스되었던 소프트웨어의 새로운 이름입니다.

- IBM Directory Server(버전 4.1 및 버전 5.1)
- IBM SecureWay Directory Server(버전 3.2.2)

IBM Directory Server 버전 4.1, IBM Directory Server 버전 5.1 및 IBM Tivoli Directory Server 버전 5.2는 모두 IBM Tivoli Access Manager 버전 5.1에 의해 지원됩니다.

IBM Tivoli Directory Server에 관한 추가 정보는 다음에서 찾을 수 있습니다.

http://www.ibm.com/software/network/directory/library/

IBM DB2 Universal Database

IBM DB2® Universal Database™ Enterprise Server Edition, 버전 8.1은 *IBM Tivoli Access Manager Directory Server* CD에서 제공되며 IBM Tivoli Directory Server 소프트웨어와 함께 설치됩니다. IBM Tivoli Directory Server, z/OS™ 또는 OS/390® LDAP 서버를 Tivoli Access Manager의 사용자 레지스트리로 사용할 경우 DB2는 필수 사항입니다.

DB2에 관한 추가 정보는 다음에서 찾을 수 있습니다.

http://www.ibm.com/software/data/db2/

IBM WebSphere Application Server

IBM WebSphere Application Server, Advanced Single Server Edition 5.0은 사용하는 운영 체제의 *IBM Tivoli Access Manager Web Administration Interfaces* CD에 포함되어 있습니다. WebSphere Application Server는 Tivoli Access Manager를 관리하는 데 사용되는 Web Portal Manager 인터페이스와 IBM Tivoli Directory Server를 관리하는 데 사용되는 웹 관리 툴을 둘 다 지원할 수 있도록 합니다. Tivoli Access Manager에는 IBM WebSphere Application Server 수정팩 2도 필요하며, 이는 *IBM Tivoli Access Manager WebSphere Fix Pack* CD에서 제공됩니다.

IBM WebSphere Application Server에 관한 추가 정보는 다음에서 찾을 수 있습니다.

http://www.ibm.com/software/webservers/appserv/infocenter.html

IBM Tivoli Access Manager for Business Integration

IBM Tivoli Access Manager for Business Integration은 별도로 주문할 수 있는 제품으로, IBM MQSeries® 버전 5.2 보안 솔루션과 IBM WebSphere® MQ 버전 5.3 메시지를 제공합니다. IBM Tivoli Access Manager for Business Integration은 송수신 어플리케이션과 연관된 키를 사용하여 WebSphere MQSeries 어플리케이션이 프라이버시와 무결성을 가지고 데이터를 송신할 수 있도록 합니다. WebSEAL 및 IBM Tivoli Access Manager for Operating Systems, IBM Tivoli Access Manager for Business Integration처럼, IBM Tivoli Access Manager의 서비스를 사용하는 자원 관리자 중 하나입니다.

IBM Tivoli Access Manager for Business Integration에 관한 추가 정보는 다음에서 찾을 수 있습니다.

http://www.ibm.com/software/tivoli/products/access-mgr-bus-integration/

IBM Tivoli Access Manager for Business Integration 버전 5.1에 대한 관련 문서는 Tivoli Information Center 웹 사이트에 있습니다.

- *IBM Tivoli Access Manager for Business Integration 관리 안내서*(SA30-1825-01)
- *IBM Tivoli Access Manager for Business Integration 문제점 판별 안내서* (GA30-2064-00)
- *IBM Tivoli Access Manager for Business Integration 설치하기 전에*(GA30-1827-01)
- *IBM Tivoli Access Manager for Business Integration Read This First* (GA30-2063-00)

IBM Tivoli Access Manager for WebSphere Business Integration Broker

IBM Tivoli Access Manager for Business Integration의 일부로 사용할 수 있는 IBM Tivoli Access Manager for WebSphere Business Integration Broker는 WebSphere Business Integration Message Broker, 버전 5.0 및 WebSphere Business Integration Event Broker, 버전 5.0에 대한 보안 솔루션을 제공합니다. IBM Tivoli Access Manager for WebSphere Business Integration Broker는 Tivoli Access Manager와 결합하여 암호 및 권한 정보 기본 인증, 중앙에서 정의된 권한 및 감사 서비스를 제공함으로써 JMS 공개/신청 어플리케이션을 보호하는 조작을 합니다.

IBM Tivoli Access Manager for WebSphere Integration Broker에 관한 추가 정보는 다음에서 찾을 수 있습니다.

http://www.ibm.com/software/tivoli/products/access-mgr-bus-integration/

IBM Tivoli Access Manager for WebSphere Integration Broker, 버전 5.1에 대한 다음 관련 문서는 Tivoli Information Center 웹 사이트에서 사용할 수 있습니다.

- *IBM Tivoli Access Manager for WebSphere Business Integration Brokers Administration Guide*(SC32-1347-00)
- *IBM Tivoli Access Manager for WebSphere Business Integration Brokers 설치하기 전에*(GA30-2194-00)
- *IBM Tivoli Access Manager for Business Integration Read This First* (GA30-2063-00)

IBM Tivoli Access Manager for Operating Systems

IBM Tivoli Access Manager for Operating Systems는 별도로 주문할 수 있는 제품으로, 기본 운영체제에서 제공하는 계층 이외에 UNIX 시스템에서 권한 부여 policy 시행 계층을 제공합니다. IBM Tivoli Access Manager for Operating Systems는 WebSEAL 및 IBM Tivoli Access Manager for Business Integration처럼 IBM Tivoli Access Manager의 서비스를 사용하는 자원 관리자 중 하나입니다.

IBM Tivoli Access Manager for Operating Systems에 관한 추가 정보는 다음에서 찾을 수 있습니다.

http://www.ibm.com/software/tivoli/products/access-mgr-operating-sys/

IBM Tivoli Access Manager for Operating Systems 버전 5.1의 다음 문서는 Tivoli Information Center 웹 사이트에 있습니다.

- *IBM Tivoli Access Manager for Operating Systems 설치 안내서*(SA30-1841-01)
- *IBM Tivoli Access Manager for Operating Systems 관리 안내서*(SA30-1840-01)
- *IBM Tivoli Access Manager for Operating Systems 문제점 판별 안내서* (SA30-1842-01)
- *IBM Tivoli Access Manager for Operating Systems 설치하기 전에*(GA30-1843-01)
- *IBM Tivoli Access Manager for Operating Systems Read Me*(GA30-1844-01)

IBM Tivoli Identity Manager

IBM Tivoli Identity Manager 버전 4.5는 별도로 주문 가능한 제품으로, 이를 사용하여 사용자(예: 사용자 ID 및 암호)를 중앙에서 관리하고 프로비저닝(즉, 어플리케이션, 자원 또는 운영 체제에 대한 액세스를 제공 또는 취소)할 수 있습니다. Tivoli Identity Manager는 Tivoli Access Manager Agent를 통해 Tivoli Access Manager와 통합할 수 있습니다. Agent 구매에 관한 자세한 정보는 IBM 담당자에게 문의하십시오.

IBM Tivoli Identity Manager에 관한 자세한 정보는 다음에서 찾을 수 있습니다.

http://www.ibm.com/software/tivoli/products/identity-mgr/

온라인 서적 액세스

제품 라이브러리의 서적은 다음 Tivoli software library에 PDF 또는 HTML 형식으로 들어 있습니다.
http://www.ibm.com/software/tivoli/library

제품 라이브러리에 액세스하려면 **Product manuals** 링크를 누르십시오. Tivoli Software Information Center에 있는 제품 이름을 찾아 누르십시오.

제품 서적은 설치하기 전에, 설치 안내서, 사용자 안내서, 관리자 안내서 및 개발자 참조서를 포함합니다.

주: PDF 문서를 인쇄할 경우, Adobe Acrobat 인쇄 대화 상자(**파일 → 인쇄**를 누르면 표시됨)에서 **페이지에 맞추기**를 선택하여 인쇄하십시오.

특수 액세스 기능

특수 액세스 기능은 거동이 불편하거나 시각 장애 등 신체적 결함이 있는 사용자가 소프트웨어 제품을 사용할 수 있도록 도와줍니다. 이 제품에서는 보조 기술을 사용하여 인터페이스의 소리를 듣고 탐색할 수 있습니다. 또한 마우스 대신 키보드를 사용하여 그래픽 사용자 인터페이스의 모든 기능을 조작할 수 있습니다.

소프트웨어 지원 문의

Tivoli 제품에 문제가 있는 경우, IBM Tivoli Software Support에 문의할 수 있습니다. 다음 웹 사이트에서 **Tivoli Support** 링크를 눌러 IBM Tivoli Software Support를 참조하십시오.
http://www.ibm.com/software/support/

지원이 필요한 경우, 다음 웹 사이트에서 *IBM Software Support Guide*에 설명한 방법을 사용하여 소프트웨어 지원에 문의하십시오.
http://techsupport.services.ibm.com/guides/handbook.html

위 서적은 문제점의 심각도에 따른 IBM Software Support에 문의하는 방법 및 다음과 같은 정보를 제공합니다.

- 등록 및 적합성
- 사용자가 속한 국가의 전화번호 및 전자 우편 주소
- 지원을 요청하기 전에 알아야 할 정보

이 책에 사용된 규칙

이 책에서는 특수 용어와 조치, 운영체제별 명령과 경로에 대해 여러 규칙을 사용합니다.

글자체 규칙

이 책에서는 다음과 같은 글자체 규칙이 사용됩니다.

굵게 텍스트 내에 표시되는 소문자 및 대소문자 혼합 명령, 키워드, 매개변수, 옵션, Java 클래스 이름 및 오브젝트는 **굵게** 표시됩니다.

기울임꼴

변수, 서적 제목, 강조하는 절이나 단어는 *기울임꼴*로 표시됩니다.

모노스페이스

텍스트 내에 표시되는 디렉토리, 파일, 출력, 명령행, 코드 예제, 시스템 메시지, 입력해야 하는 텍스트 및 인수값 또는 명령 옵션은 모노스페이스로 표시됩니다.

운영체제에 따른 변수 및 경로

이 책에서는 디렉토리 표기 및 환경 변수 지정에 UNIX 규칙을 사용합니다. Windows 명령을 사용할 경우는, 환경 변수의 *$variable*을 *%variable%*로 바꾸고, 디렉토리 경로의 슬래시(/)를 백슬래시(\)로 바꾸십시오. Windows 시스템에서 bash 쉘을 사용할 경우, UNIX 규칙을 사용하십시오.

제 1 장 소개 및 개요

Tivoli Access Manager for WebLogic은 Tivoli Access Manager의 보안 기능을 사용하여 BEA WebLogic Server 어플리케이션에 대한 액세스를 보호하는 Tivoli Access Manager에 대한 확장입니다. BEA WebLogic Server Security Service Provider Interface를 사용할 경우, Tivoli Access Manager for WebLogic은 Tivoli Access Manager가 관리하는 사용자 레지스트리를 사용하여 클라이언트를 인증합니다. IBM Tivoli Access Manager WebSEAL(WebSEAL) 또는 IBM Tivoli Access Manager Plug-in for Web Server를 사용하여 일반 사용자 싱글 사인 온에 대한 지원을 제공하도록 Tivoli Access Manager for WebLogic의 보안 기능을 확장할 수 있습니다.

Tivoli Access Manager for WebLogic을 사용하여 WebLogic 서버 어플리케이션은 코딩 또는 배치를 변경할 필요없이 Tivoli Access Manager 보안을 사용할 수 있습니다.

Tivoli Access Manager for WebLogic을 설치하기 전에 Tivoli Access Manager 보안 도메인을 배치해야 합니다.

Tivoli Access Manager에 익숙하지 않은 사용자는 보안 도메인을 배치하기 전에 Tivoli Access Manager 보안 모델을 검토해야 합니다. 여기에는 보안 모델에 대한 간단한 요약이 제공됩니다.

Tivoli Access Manager 보안 모델

Tivoli Access Manager는 지역적으로 분산된 인트라넷 및 익스트라넷에 있는 자원을 철저하게 보호해 주는 완전한 권한 및 네트워크 보안 policy 관리 솔루션입니다.

Tivoli Access Manager는 최첨단의 보안 policy 관리를 제공합니다. 또한 인증, 권한, 데이터 보안, 자원 관리 기능을 지원합니다. Tivoli Access Manager를 표준 인터넷 기반 어플리케이션과 함께 사용하여 매우 안전하고 잘 관리되는 인트라넷 및 익스트라넷을 빌드할 수 있습니다.

Tivoli Access Manager는 다음을 제공합니다.

- 인증 프레임워크

  Tivoli Access Manager는 인증, 기본 인증, 양식 및 HTTP 헤더를 포함한 광범위한 인증 메커니즘을 지원합니다.

- 권한 프레임워크

  Tivoli Access Manager는 권한 policy 관리를 위한 프레임워크를 제공합니다. 권한 policy는 중앙에서 관리되며 엔터프라이즈 전체의 액세스 적용 지점으로 자동 분배

© Copyright IBM Corp. 2003

됩니다. Tivoli Access Manager 권한 서비스는 원시 Tivoli Access Manager 서버 및 서드파티(third-party) 어플리케이션의 액세스 요청에 대한 *허용* 및 *거부*를 결정합니다.

WebSEAL은 웹 기반 자원에 대한 Tivoli Access Manager 자원 보안 관리자입니다. WebSEAL은 보호 웹 자원에 세분화된 보안을 적용하는 고성능 멀티스레드 웹 서버입니다.

Tivoli Access Manager Plug-in for Web Servers는 Tivoli Access Manager와 통합하여 웹 자원의 전체 보안 솔루션을 제공합니다. 이 플러그인은 웹 서버와 동일한 프로세스의 파트로 조작하여 도착하는 각 요청을 인터셉트하고 권한 결정이 필요한지 여부를 결정하며 필요하면 사용자 인증 수단을 제공합니다.

Tivoli Access Manager Plug-in for Web Servers 및 WebSEAL을 둘다 싱글 사인온 솔루션을 제공하고 웹 어플리케이션 자원을 자신의 보안 policy에 통합시킬 수 있습니다.

IBM Tivoli Access Manager에 대한 문서를 검토하여 배치 결정을 내리는 데 필요한 정보를 포함하여 Tivoli Access Manager에 대해 더 자세하게 배울 수 있습니다. 이 책의 서문에는 관련 Tivoli Access Manager 문서의 목록이 포함되어 있습니다.

Tivoli Access Manager 및 WebLogic 서버 통합

Tivoli Access Manager for WebLogic, 버전 5.1은 다음을 지원합니다.

- BEA WebLogic Server 버전 7.0 SP2
- BEA WebLogic Server 버전 8.1 SP1

Tivoli Access Manager for WebLogic 버전 5.1은 SSPI(Security Service Provider Interface)를 사용하여 BEA WebLogic Server에 대한 전체 보안 프레임워크를 제공합니다.

주: Tivoli Access Manager for WebLogic 버전 5.1은 BEA WebLogic Server 사용자 정의 범위를 지원하지 않습니다. BEA WebLogic Server 사용자 정의 범위에 대한 지원은 Tivoli Access Manager for WebLogic 버전 4.1의 파트입니다.

BEA WebLogic Server는 서드파티(thrid-party) 보안 제공자(예: Tivoli Access Manager for WebLogic)의 SSPI를 제공하여 자신의 보안 기능을 BEA WebLogic Server 구조에 완전히 통합시킵니다.

Tivoli Access Manager Security Service Provider Interface 구성요소

Tivoli Access Manager for WebLogic은 작성된 기본 보안 범위를 각 BEA WebLogic Server 보안 도메인과 바꾸고 다음과 같은 BEA WebLogic Server 보안 제공자를 제공합니다.

- 인증 제공자
- 권한 제공자
- 역할 맵핑 제공자

Tivoli Access Manager for WebLogic은 기본 BEA WebLogic Server 권한 정보 맵핑 보안 제공자 및 기본 키스토어를 사용합니다.

위에 나열된 각 제공자는 또한 WebLogic 콘솔을 통해 구성 편집을 할 수 있게 하는 Management Bean(MBean)을 포함합니다. 아래의 절에서는 이들 각 제공자 및 MBean이 제공하는 기능에 대해 자세히 설명합니다.

Tivoli Access Manager는 다음 통합 지점에 BEA WebLogic Server를 제공합니다.

인증 제공자

Tivoli Access Manager for WebLogic 인증 제공자는 BEA WebLogic Server 단순 인증을 구현합니다. 단순 인증에서 사용자는 사용자 이름 및 암호 조합을 사용하여 BEA WebLogic Server에 대해 인증하려는 시도를 합니다. Tivoli Access Manager는 Tivoli Access Manager Java 런타임 구성요소를 사용하여 이 사용자 이름 및 암호를 점검합니다.

Tivoli Access Manager for WebLogic은 또한 WebSEAL 또는 Tivoli Access Manager Plug-in for Web Servers 싱글 사인 온 기능을 제공하는 데 사용되는 자체 로그인 모듈을 제공합니다. 싱글 사인 온 기능 사용 가능에 대한 세부사항은 37 페이지의 제 4 장『싱글 사인 온 사용 가능』에 포함되어 있습니다.

Tivoli Access Manager for WebLogic에 대한 인증 제공자는 여러 구성요소로 이루어져 있습니다.

- 인증 제공자

  IBM Tivoli Access Manager for WebLogic Server 인증 제공자를 WebLogic 보안 프레임워크에 통합시킵니다.

- JAAS(Java Authentication and Authorization Service) 로그인 모듈

  단순 및 싱글 사인 온 인증을 수행합니다. JAAS 로그인 모듈은 JAAS 표준이 지정한 프린시펄(사용자)로 채워진 주제를 리턴합니다. Tivoli Access Manager for

WebLogic은 자체 로그인 모듈을 제공하는데, 이 모듈은 Tivoli Access Manager Java 런타임 구성요소를 사용하여 Tivoli Access Manager Authorization Server에 대해 인증합니다.

- 인증 MBean

  WebLogic 콘솔을 통해 인증 제공자를 구성할 수 있도록 합니다. 또한 사용자가 Tivoli Access Manager for WebLogic 콘솔 확장을 사용하여 사용자를 추가하고 삭제하는 것과 같은 사용자 레지스트리 관리 태스크를 수행할 수 있도록 합니다.

권한 제공자

권한 제공자는 BEA WebLogic Server와 외부 권한 서비스 간의 인터페이스를 제공합니다. 권한 제공자는 BEA WebLogic Server 자원에 대한 액세스가 허용되는지 또는 거부되는지 여부를 판별합니다. 액세스 결정은 Tivoli Access Manager Java 런타임 구성요소를 사용하여 분배된 PDPermission 클래스를 사용하여 작성됩니다.

Tivoli Access Manager for WebLogic에 대한 권한 제공자는 다음 구성요소로 이루어져 있습니다.

- 권한 제공자

  권한 제공자를 WebLogic 보안 프레임워크에 통합시킵니다. Tivoli Access Manager for WebLogic 권한 제공자는 BEA WebLogic Server 자원에 대한 액세스를 제어할 뿐만 아니라 Tivoli Access Manager 오브젝트 공간에 policy 배치 및 Tivoli Access Manager 오브젝트 공간에서 policy 제거를 처리합니다.

- 권한 MBean

  WebLogic 콘솔을 통해 권한 제공자를 구성할 수 있도록 합니다. WebLogic 콘솔을 통한 policy 작성 및 삭제와 같은 조작을 하도록 호출될 수도 있습니다.

역할 맵핑 제공자

역할 맵핑 제공자는 역할을 관리하는 데 사용되는 BEA WebLogic Server와 외부 권한 서비스 간의 인터페이스를 제공하는 데 사용됩니다. 역할 맵핑 제공자는 권한 제공자의 책임인 policy보다는 역할에 중점을 둡니다.

역할 맵핑 제공자는 다음과 같은 구성요소로 이루어져 있습니다.

- 역할 맵핑 제공자

  역할 맵핑 제공자를 WebLogic 보안 프레임워크에 통합시킵니다. Tivoli Access Manager for WebLogic 역할 맵핑 제공자는 역할의 배치 및 제거에 대한 책임을 가집니다.

- 역할 맵핑 MBean

  WebLogic 콘솔을 통해 역할 맵핑 제공자를 구성할 수 있도록 합니다. WebLogic 콘솔을 통해 역할을 삭제하여 역할 구성원을 작성 및 갱신하는 것과 같은 조작을 하도록 호출될 수도 있습니다.

Policy 및 역할 배치

Policy 및 역할을 배치 디스크립터에 정의하거나 WebLogic 콘솔을 통해 작성할 수 있습니다. J2EE 어플리케이션의 배치 시, 어플리케이션 배치 디스크립터 내에 정의된 역할 및 policy는 Tivoli Access Manager 보호 오브젝트 공간으로 반출됩니다.

Tivoli Access Manager 관리 유틸리티인 **pdadmin** 또는 Tivoli Access Manager Web Portal Manager를 사용하여 policy를 작성할 수는 있으나 수행할 수는 없습니다. Tivoli Access Manager for WebLogic을 사용하는 BEA WebLogic Server를 시작하기 전에 Tivoli Access Manager에 몇 가지 기본 policy가 작성되어야 합니다. 이는 Tivoli Access Manager for WebLogic 구성 중 수행됩니다. Tivoli Access Manager for WebLogic 구성에 대한 세부사항은 23 페이지의 제 3 장『구성 절차』에 나와 있습니다.

자원 및 역할

BEA WebLogic Server는 여러 개의 서로 다른 자원 유형을 정의하며, 모두 Tivoli Access Manager for WebLogic에 의해 지원됩니다. 모든 자원 유형은 Tivoli Access Manager for WebLogic 내에서 동일한 것으로 간주되므로, BEA WebLogic Server의 향후 릴리스용으로 작성된 새 자원 유형도 자동으로 지원됩니다.

모든 자원 유형에 대해 정의된 policy 및 역할은 Tivoli Access Manager 보호 오브젝트 공간에 동일한 방식으로 저장됩니다.

현재 보호되지 않고 지원되는 BEA WebLogic Server 자원 목록은 다음과 같습니다.

- 관리 자원
- 어플리케이션 자원
- COM 자원
- EIS 자원
- EJB 자원
- JDBC 자원
- JMS 자원
- 서버 자원
- URL 자원
- 웹 서비스 자원

Tivoli Access Manager 보호 오브젝트 공간에서 자원은 다음 형식으로 표시됩니다.

`/WebAppServer/WLS/Resources/`*`wls_domain`*`/`*`wls_realm`*`/`*`resource_type`*`/Details`

Tivoli Access Manager 보호 오브젝트 공간에서 역할은 다음 형식으로 표시됩니다.

`/WebAppServer/WLS/Roles/`*`wls_domain`*`/`*`wls_realm`*`/`*`role_name`*`/AppName`

이들 Tivoli Access Manager 보호 오브젝트 컨테이너 이름은 Tivoli Access Manager for WebLogic으로 구성된 특성 파일을 사용하여 완전히 구성될 수 있습니다. 따라서 모든 BEA WebLogic Server 및 기타 어플리케이션 서버를 동일한 Tivoli Access Manager 도메인 내에 구성할 수 있습니다. 이는 모든 어플리케이션 서버 유형의 역할 및 policy에 대한 집중된 위치를 작성할 수 있도록 합니다.

Tivoli Access Manager 인증 사용

Tivoli Access Manager를 사용하여 외부 사용자 또는 내부 사용자에 대한 인증을 제공할 수 있습니다. 외부 사용자에 대한 인증은 WebSEAL 또는 Tivoli Access Manager Plug-in for Web Servers의 싱글 사인 온 기능에 의존합니다. 최적의 네트워크 보안을 위해 WebSEAL 또는 Tivoli Access Manager Plug-in for Web Servers를 통해 외부 사용자의 액세스 요청을 수신하는 각 WebLogic 서버는 내부 사용자의 액세스 요청을 채택하지 말아야 합니다. 다음 절에서는 외부 사용자와 내부 사용자 모두에 대해 인증을 처리하는 방법에 대해 설명합니다.

WebSEAL을 사용하여 외부 사용자 인증

아래 다이어그램은 보호 자원에 액세스하려는 외부 사용자의 요청을 처리하는 모델을 보여줍니다.

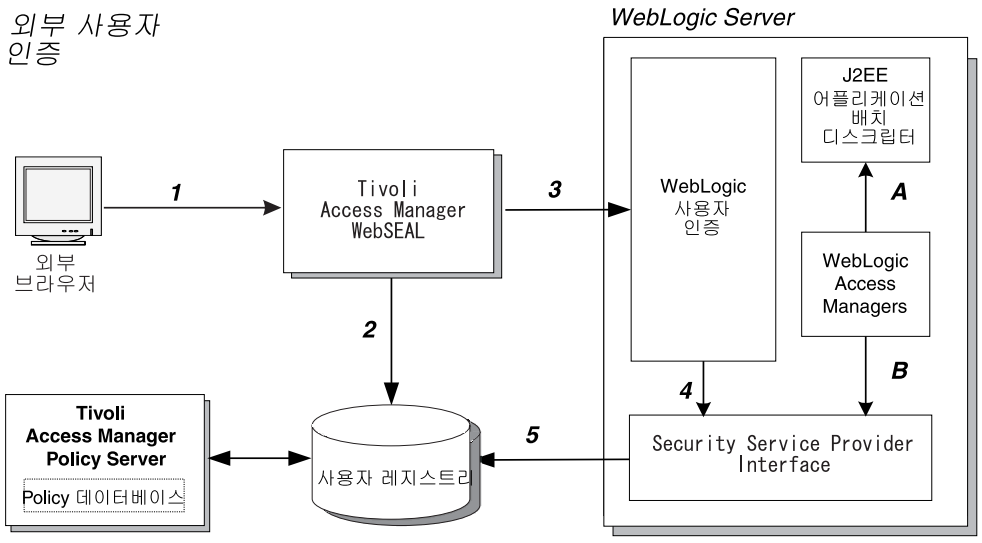

그림 1. Tivoli Access Manager는 외부 사용자에 대한 싱글 사인 온 인증을 제공합니다.

다음 목록에서는 위의 그림에 표시된 프로세스에 대해 설명합니다.

1. 외부 사용자가 보호 자원에 대한 액세스를 요청합니다. WebSEAL은 엔터프라이즈의 보안 네트워크에 들어가기 전에 요청을 수신합니다
2. WebSEAL은 사용자의 요청을 인터셉트하여 Tivoli Access Manager 보안 도메인에서 해당 사용자를 인증합니다.

WebSEAL은 사용자 이름 및 암호, 인증서, 사용자 이름 및 RSA SecureID 또는 사용자 정의 인증 메커니즘의 인증 메소드를 지원합니다.

WebSEAL은 요청된 URL 및 Tivoli Access Manager 액세스 policy에 따라 자체 권한 결정을 적용합니다. WebSEAL은 고려사항(예: 계정 유효성, 시간 및 인증 메커니즘)을 적용할 수 있습니다.

3. 사용자의 URL 요청이 권한 부여된 후, WebSEAL은 이를 WebLogic 서버로 전달합니다. 요청에는 외부 사용자 이름과 기본 인증 헤더 내의 특수 암호가 포함됩니다. 특수 암호는 *sso_user*에 속하며 Security Service Provider Interface가 WebSEAL을 요청 오리진으로 확인할 수 있도록 합니다.

   *sso_user*에 대한 자세한 정보는 23 페이지의 제 3 장『구성 절차』를 참조하십시오.

4. WebLogic 서버는 인증된 사용자 ID와 암호를 Security Service Provider Interface로 투명하게 전달합니다.
5. Security Service Provider Interface는 Tivoli Access Manager 인증 서비스를 사용하여 WebSEAL이 제공한 암호가 위에 설명된 *sso_user*에 대해 올바른 암호인지 검증합니다. 즉, 이 암호는 요청 오리진이 WebSEAL이라는 신뢰를 기초로 합니다

이제 권한에 대한 요청이 준비되었습니다.

내부 사용자 인증

아래의 다이어그램에서는 *내부* 사용자가 WebSEAL 또는 플러그인 보안을 통하지 않고 보호 자원에 액세스하기 위한 요청을 처리하는 모델을 보여줍니다.

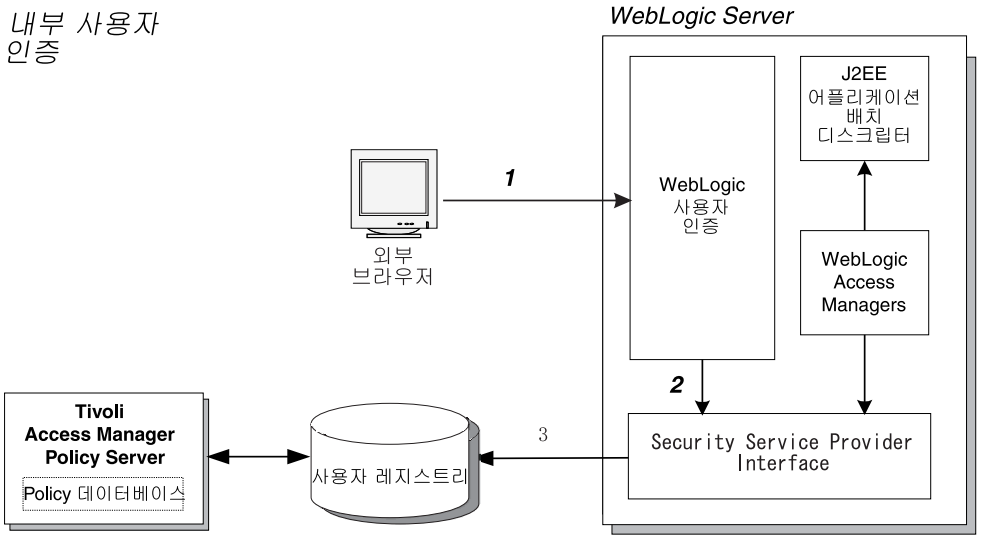

그림 2. Tivoli Access Manager Custom Realm은 내부 사용자의 인증을 제공합니다.

다음 목록에서는 위의 그림에 표시된 프로세스에 대해 설명합니다.

1. 내부 사용자가 보호 자원에 대한 액세스를 요청합니다.
2. WebLogic 사용자 인증 모듈이 사용자의 ID를 Security Service Provider Interface로 보냅니다.
3. Security Service Provider Interface는 인증 요청을 사용자 레지스트리로 보냅니다.

   인증이 완료되면, Security Service Provider Interface는 이 사용자 이름을 인증된 사용자로서 WebLogic 서버로 리턴합니다.
4. 요청을 권한 부여하기 위해 BEA WebLogic Server는 현재 인증된 사용자(아마도 권한이 부여되지 않은)가 요청된 자원에 액세스할 수 있도록 권한이 부여되었는지 여부를 판별하는 Tivoli Access Manager for WebLogic 권한 제공자에게 조회합니다.

   액세스는 자원에 대한 액세스가 부여된 역할을 선택하고 현재 인증된 사용자가 이러한 역할이 부여되었는지 여부를 결정하는 Tivoli Access Manager Authorization Server에게 호출하여 판별됩니다.

로깅 및 감사

Tivoli Access Manager for WebLogic 내에서 로깅은 Tivoli Access Manager Java 런타임 구성요소를 사용하여 분배된 IBM JLog 클래스에 의해 처리됩니다. Tivoli Access Manager for WebLogic 및 Tivoli Access Manager for WebLogic과 함께 공급된 JLog *특성* 파일을 BEA WebLogic Server 로깅 클래스를 사용하도록 구성할 수 있습니다. 이렇게 하면 Tivoli Access Manager for WebLogic이 WebLogic 로그 파일에 이벤트를 직접 로그할 수 있습니다.

신뢰성, 가용성, 크기 조정 가능성

Tivoli Access Manager for WebLogic은 Tivoli Access Manager Java 런타임 클래스를 사용하여 Tivoli Access Manager 보호 오브젝트 데이터베이스 및 사용자 레지스트리를 조작합니다. 내부 Tivoli Access Manager for WebLogic 캐시는 액세스 결정에 대한 성능 향상을 제공합니다.

Tivoli Access Manager Java 런타임 클래스는 Tivoli Access Manager Authorization Server 오류 복구를 지원합니다. 1차 Authorization Server가 손상될 경우, 2차 서버에 대한 오류 복구가 자동 발생합니다.

권장되는 환경 설정은 복제 **acld** 및 Tivoli Access Manager for WebLogic 인타이틀먼트 서비스를 사용하는 것입니다.

액세스 결정은 Tivoli Access Manager for WebLogic과 함께 제공되는 Tivoli Access Manager Authorization Server 인타이틀먼트 서비스 또는 Tivoli Access Manager Policy Server를 사용하여 수행할 수 있습니다.

Tivoli Access Manager Policy Server 구성은 실패 및 성능의 단일 지점 문제 때문에 테스트 환경에서만 사용해야 합니다. 인타이틀먼트 서비스는 프로덕션 환경에서 사용되도록 특정하게 개발되었습니다. 자세한 내용은 39 페이지의 『Tivoli Access Manager Authorization Server에서 인타이틀먼트 서비스 사용』을 참조하십시오.

제 2 장 설치 지시사항

이 장은 다음 주제로 구성되어 있습니다.

- 『지원되는 플랫폼』
- 『디스크 및 메모리 요구사항』
- 12 페이지의 『사전 설치 소프트웨어』
- 14 페이지의 『설치 마법사를 사용하여 설치』
- 17 페이지의 『원시 유틸리티를 사용하여 설치』

지원되는 플랫폼

Tivoli Access Manager for WebLogic, 버전 5.1은 다음을 지원합니다.

- BEA WebLogic Server 버전 7.0 SP2
- BEA WebLogic Server 버전 8.1 SP1

Tivoli Access Manager for WebLogic은 이 릴리스에 대한 사용자 정의 범위를 지원하지 않습니다. 대신, 이 통합은 BEA WebLogic Server SSPI(Security Service Provider Interface)를 지원합니다.

Tivoli Access Manager for WebLogic은 다음 운영 체제에서 지원됩니다.

- IBM AIX 5.1
- Sun Solaris 8 및 9
- Hewlett-Packard HP-UX 11.0 및 11i(BEA WebLogic Server 버전 7.0만)
- Microsoft Windows 2000 Server 및 Advanced Server(서비스 팩 3)

주: Tivoli Access Manager for WebLogic은 Java 2 Security Manager를 사용하여 실행하는 시스템을 지원합니다. Java policy 파일은 Java 2 Security Manager의 특정 코드베이스가 작업하는 데 필요한 권한을 포함하는 소프트웨어와 함께 제공됩니다.

디스크 및 메모리 요구사항

Tivoli Access Manager for WebLogic의 디스크 및 메모리 요구사항은 다음과 같습니다.

- 64MB RAM, 128MB 권장됨

© Copyright IBM Corp. 2003

BEA WebLogic Server 및 기타 Tivoli Access Manager 구성요소에 지정된 필수 메모리 이외에 필요한 메모리 양입니다. 추가 64MB RAM은 캐싱 성능을 최적화하는 데 사용됩니다.

다른 Tivoli Access Manager 구성요소에 필요한 메모리 양은 호스트 시스템에 설치된 Tivoli Access Manager 구성요소에 따라 달라집니다. 자세한 정보는 *IBM Tivoli Access Manager 기본 설치 안내서*를 참조하십시오.

- 2MB 디스크 공간, 4MB 권장됨

  BEA WebLogic Server 및 기타 Tivoli Access Manager 구성요소에 필요한 디스크 공간 이외에 추가로 필요한 공간입니다.

- 로그 파일에 대해 5MB 디스크 공간

  이는 소프트웨어 구성요소에 필요한 디스크 공간 이외에 추가로 필요한 공간입니다.

사전 설치 소프트웨어

Tivoli Access Manager for WebLogic의 설치를 완료하려면 다음과 같은 사전 설치 소프트웨어가 필요합니다.

- 『Tivoli Access Manager Policy Server』
- 13 페이지의 『Tivoli Access Manager WebSEAL 또는 Tivoli Access Manager Plug-in for Web Servers』
- 13 페이지의 『BEA WebLogic Server』
- 14 페이지의 『Tivoli Access Manager Java 런타임』

Tivoli Access Manager Policy Server

Tivoli Access Manager for WebLogic을 설치하기 전에 Tivoli Access Manager 보안 도메인을 설정해야 합니다.

Tivoli Access Manager Policy Server를 설치할 때 Tivoli Access Manager 보안 도메인이 설정됩니다. 이 Policy Server는 사용자 운영 체제의 IBM Tivoli Access Manager Base CD에서 배포됩니다.

일반적으로 Tivoli Access Manager Policy Server는 Tivoli Access Manager for WebLogic을 담당하는 시스템과 다른 시스템에 설치됩니다.

Tivoli Access Manager Authorization Server

Tivoli Access Manager Authorization Server는 BEA WebLogic Server 및 Tivoli Access Manager for WebLogic이 설치된 것과 동일한 호스트에 설치되어야 합니다.

Authorization Server는 BEA WebLogic Server에 Tivoli Access Manager 권한 서비스에 대한 액세스를 제공합니다. Authorization Server는 또한 서버 활동 레코드를 저장하기 위한 로깅 및 감사 콜렉션 서버 역할을 합니다.

Tivoli Access Manager WebSEAL 또는 Tivoli Access Manager Plug-in for Web Servers

Tivoli Access Manager WebSEAL(WebSEAL) 및 Tivoli Access Manager Plug-in for Web Servers(플러그인)은 Tivoli Access Manager for WebLogic이 사용할 수 있는 웹 기반 보안 서비스를 제공합니다. 이들 어플리케이션이 설치 완료되면 BEA WebLogic Server 싱글 사인 온 솔루션을 제공하는 데 사용할 수 있습니다.

WebSEAL 또는 플러그인은 Tivoli Access Manager for WebLogic을 설치하기 위한 사전 설치 소프트웨어가 아닙니다. 그러나 싱글 사인 온 솔루션을 요구할 경우에는 필요합니다.

WebSEAL 또는 플러그인에 대한 설치 지시사항에 대해서는 *IBM Tivoli Access Manager for e-business 웹 보안 설치 안내서*를 참조하십시오.

WebSEAL 또는 기타 프록시 서버를 사용하여 BEA WebLogic Server에 연결할 경우, 이 프록시 서버가 BEA WebLogic Server 보호 자원에 액세스하는 사용자의 단일 연락 지점인지 확인해야 합니다. 액세스를 제한하려면 BEA WebLogic Server 연결 필터를 작성해야 합니다. 연결 필터를 사용하면 액세스를 제한하기 위한 역할을 사용하는 대신 네트워크 레벨에서 자원을 보호할 수 있습니다. 연결 필터 작성에 대한 자세한 내용은 BEA WebLogic Server 문서를 참조하십시오.

BEA WebLogic Server

Tivoli Access Manager for WebLogic을 호스트할 시스템에 BEA WebLogic Server가 설치 및 구성되어야 합니다. BEA WebLogic Server는 **startWebLogic** 명령을 사용하여 시작합니다.

BEA WebLogic Server는 AIX를 제외한 모든 지원 플랫폼에 필요한 Java Runtime Environment와 함께 분배됩니다. Tivoli Access Manager for WebLogic은 동일한 JRE(Java Runtime Environment)를 사용합니다. BEA WebLogic Server의 설치를 완료하면 JRE에 대한 Tivoli Access Manager for WebLogic 전제조건을 충족시킵니다.

AIX의 IBM Java Runtime Environment

AIX 시스템에서 BEA WebLogic Server 7.0을 사용하려면 Tivoli Access Manager for WebLogic을 호스트할 시스템에 IBM Java Runtime Environment 버전 1.3이 설치되어야 합니다. AIX 시스템에서 BEA WebLogic Server 8.1을 사용하려면 Tivoli Access Manager for WebLogic을 호스트할 시스템에 IBM Java Runtime Environment 버전 1.4가 설치되어야 합니다. Tivoli Access Manager for WebLogic은 이들 동일한 버전의 Java Runtime Environment를 사용합니다.

Tivoli Access Manager Java 런타임

Tivoli Access Manager for WebLogic을 호스트할 시스템에 Tivoli Access Manager 기본의 Tivoli Access Manager Java 런타임 버전 5.1 환경을 설치 및 구성해야 합니다.

Tivoli Access Manager Java 런타임 환경은 Java 기반 인증 및 권한 기능을 제공합니다. Java 클래스는 BEA WebLogic Server가 사용하는 JRE(Java Runtime Environment)를 확장합니다.

Tivoli Access Manager for WebLogic을 호스트할 시스템에 Tivoli Access Manager Java Runtime Environment를 구성하기 전에 Tivoli Access Manager 보안 도메인을 확립해야 합니다.

Tivoli Access Manager Java Runtime Environment는 각 지원되는 운영 체제에 대한 IBM Tivoli Access Manager Base CD에 의해 분배됩니다. 설치에 대한 자세한 내용은 *IBM Tivoli Access Manager 기본 설치 안내서*를 참조하십시오.

설치 마법사를 사용하여 설치

> **주의**
>
> 이 설치 마법사는 BEA WebLogic Server, 버전 7.0의 기본 설치 위치에 대해서만 지원됩니다. BEA WebLogic Server, 버전 8.1을 사용하는 경우, 17 페이지의 『원시 유틸리티를 사용하여 설치』의 지시사항을 따르십시오.

install_amwls 설치 마법사는 다음 구성요소를 적절한 순서로 설치하고 구성하여 Tivoli Access Manager for WebLogic Server 시스템의 설정을 단순화시킵니다.

- Access Manager Java Runtime Environment
- Access Manager for WebLogic Server

install_amwls 마법사를 사용하여 Tivoli Access Manager for WebLogic Server 시스템을 설치하고 구성하려면 다음 단계를 따르십시오.

1. Tivoli Access Manager 레지스트리 서버, Policy Server 및 Authorization Server를 이미 도메인에 설정했는지 확인하십시오.
2. 모든 필요한 운영 체제 패치가 설치되었는지 확인하십시오. 자세한 정보는 11 페이지의 『지원되는 플랫폼』을 참조하십시오.
3. 영어(기본값) 이외의 다른 언어로 상태 및 메시지를 보려면 설치 마법사를 실행하기 *전에* 언어 지원 패키지를 설치해야 합니다.
4. 이 시스템에 BEA WebLogic Server가 설치 및 구성되어 있고 BEA WebLogic Server 도메인이 작성되었는지 확인하십시오.

5. Windows 시스템에서 실행 중인 모든 프로그램을 종료하십시오.
6. BEA WebLogic Server를 시작하십시오.

   UNIX */WLS_install_dir*/user_projects/*domain_name*/
   startWebLogic.sh

   Windows

   C:*WLS_install_dir*\user_projects*domain_name*/
   startWebLogic.cmd

7. BEA WebLogic Server *WebLogic_install_dir*/server/bin 디렉토리에서 다음 스크립트를 실행하여 CLASSPATH 및 PATH 변수를 설정한 후 WebLogic .jars를 CLASSPATH, bin 및 lib 디렉토리에 추가하십시오.

   UNIX .setWLSEnv.sh

   Windows

   setWLSEnv.cmd

   설치 마법사를 실행하기 전에 BEA WebLogic Server와 함께 제공된 Java 실행 파일이 시스템 경로에서 맨 앞에 있는지 확인하십시오.
8. AIX, HP-UX(BEA WebLogic Server 7.0만), Solaris 및 Windows 플랫폼용 Tivoli Access Manager Web Security CD의 루트 디렉토리에 있는 **install_amwls** 프로그램을 실행하십시오. BEA WebLogic Server가 기본 위치에 설치되어 있지 않으면, 다음 명령을 사용하여 설치 마법사를 실행해야 합니다.

   install_amwls -is:javahome *path*

   여기서 *path*는 마법사를 사용한 설치를 수행하는 데 사용되는 jre의 위치입니다.

   주:

   a. 간단히 기본 설치 값을 겹쳐쓰거나 자동 설치를 위해 install_amwls.options.template 파일을 사용할 수 있습니다. 필요한 모든 값을 포함시키려면 간단히 파일을 편집하십시오.
      - 기본값을 겹쳐쓰려면 다음 명령을 사용하십시오.

        install_amwls -options install_amwls.options.template
      - 자동 설치를 수행하려면 다음을 사용하십시오.

        install_amwls -silent -options install_amwls.options.template

   b. BEA WebLogic Server와 함께 제공되는 JDK를 사용할 때 비영어 플랫폼의 설치 마법사는 시작 화면에 일관되지 않는 텍스트를 표시할 수 있습니다. 이 표시 문제는 실제 소프트웨어 설치에 영향을 주지 않습니다. 이 문제점을 정정하려면, IBM JDK 1.3.1을 설치하고 이를 사용하여 **install_amwls**를 실행하십시오.

설치 마법사가 시작되어 16 페이지의 『install_amwls 옵션』에 설명된 대로 구성 정보에 대한 프롬프트를 표시합니다. 단 Windows 시스템에서는 Tivoli Access Manager for WebLogic에 대해 기본 설치 디렉토리를 채택해야 합니다.

주: 이 정보를 제공하면(또는 기본값을 채택하면), 더 이상 개입되지 않고 구성요소가 설치되고 구성됩니다.

설치 마법사의 맨 끝에는 설치된 구성요소, 시도된 구성사항 및 완료 여부를 보여주는 요약 화면이 표시됩니다. 설치가 완료되었지만 구성이 실패된 경우, 23 페이지의 제 3 장 『구성 절차』의 단계에 따라 Tivoli Access Manager for WebLogic을 수동으로 구성하거나 다음 단계를 계속 수행할 수 있습니다.

9. BEA WebLogic Server를 중지하십시오.
10. 설치 프로그램이 AMSSPIProviders.jar 파일을 */bea_install_dir*/weblogic/server/lib/mbeantypes 디렉토리에 복사했는지 점검하십시오. 이 디렉토리에 해당 파일이 존재하지 않을 경우, */amwls_install_dir*/lib에서 수동으로 파일을 복사하십시오.
11. 25 페이지의 『제 2 부: startWebLogic에 대한 CLASSPATH 설정』의 지시사항에 따라 startWebLogic 명령에 대한 CLASSPATH를 설정하십시오.
12. Tivoli Access Manager 범위를 작성하여 구성하십시오. 지시사항에 대해서는 29 페이지의 『제 4 부: Tivoli Access Manager 범위 구성』을 참조하십시오.
13. WebLogic 콘솔을 사용하여 BEA WebLogic Server를 다시 시작하십시오.
14. Tivoli Access Manager WebSEAL을 사용하여 BEA WebLogic Server에 대한 싱글 사인 온 서비스를 제공하려면 32 페이지의 『제 5 부: BEA WebLogic Server 싱글 사인 온 구성』의 지시사항에 따르십시오.
15. 34 페이지의 『제 7 부: 구성 테스트』의 단계를 완료하여 설치 및 구성을 테스트함으로써 Tivoli Access Manager for WebLogic이 Tivoli Access Manager 레지스트리에 대해 올바로 구성되었는지 확인하십시오.

install_amwls 옵션

install_amwls를 실행할 때 다음 옵션이 표시됩니다.

표 1. **install_amwls** *설치 마법사 구성 옵션*

구성 옵션	설명	기본값
원격 ACL 사용자*	Authorization Server와 통신하기 위해 작성된 Tivoli Access Manager 프린시펄(사용자)	
sec_master 암호*	Tivoli Access Manager 관리자 암호	
Policy Server 호스트 이름*	Policy Server의 완전한 호스트 이름. 예를 들면, 다음과 같습니다. pdmgr.tivoli.com	

표 1. **install_amwls** *설치 마법사 구성 옵션 (계속)*

Policy Server 포트 번호*	Policy Server가 요청을 인식하는 포트 번호. 기본 포트 번호는 **7135**입니다.	7135
Authorization Server 호스트 이름*	Tivoli Access Manager Authorization Server 호스트 이름	
Authorization Server 포트 번호*	Authorization Server 포트 번호	7136
True로 설정할 경우 AMWLS5.1 콘솔 확장 배치		true
WebLogic 도메인 관리자*	BEA WebLogic Server 도메인의 관리자. 이 사용자는 WebLogic 도메인을 작성할 때 확립되었습니다.	
WebLogic 도메인 관리 암호*	WebLogic 도메인 관리자의 암호	
Access Manager for WebLogic Server 설치 디렉토리 경로	*Windows 시스템에서는 기본값을 사용해야 합니다.*	`C:\Program Files\Tivoli\pdwls`
WebLogic Admin Server의 URL		`t3://localhost:7001`

원시 유틸리티를 사용하여 설치

운영 체제에 따라 해당 절에 있는 지시사항을 따르십시오.

- 『AIX에 설치』
- 18 페이지의 『HP-UX에 설치』
- 19 페이지의 『Solaris에 설치』
- 20 페이지의 『Windows에 설치』

주: Tivoli Access Manager for WebLogic을 설치하기 전에 반드시 BEA WebLogic Server를 중지한 후 설치가 완료되면 다시 시작하십시오.

AIX에 설치

Tivoli Access Manager for WebLogic을 설치하면 패키지 구성에서 파일이 추출됩니다. AIX에 소프트웨어 패키지를 설치하려면 **installp**를 사용하십시오. 그런 다음 Tivoli Access Manager for WebLogic을 수동으로 구성하십시오.

주: Tivoli Access Manager for WebLogic을 이미 설치 및 구성한 상태에서 다시 설치해야 할 경우, 우선 이를 구성 해제한 다음 제거해야 합니다. 50 페이지의 『AIX에서 제거』를 참조하십시오.

AIX에 Tivoli Access Manager for WebLogic을 설치하려면 다음 지시사항을 완료하십시오.

1. *root*로 로그인하십시오.
2. Tivoli Access Manager 기본의 필수 구성요소를 포함한 사전 설치 소프트웨어가 설치되어 있는지 확인하십시오. 12 페이지의 『사전 설치 소프트웨어』를 참조하십시오.

3. *IBM Tivoli Access Manager Web Security for AIX* CD를 CD 드라이브에 넣으십시오.
4. 쉘 프롬프트에 다음 명령을 입력하십시오.

   ```
   installp -acgNXd cd_mount_point/usr/sys/inst.images PDWLS
   ```

   주: 설치 프로그램이 AMSSPIProviders.jar 파일을 */bea_install_dir/*weblogic/server/lib/mbeantypes 디렉토리에 복사했는지 점검하십시오. 이 디렉토리에 해당 파일이 존재하지 않을 경우 */amwls_install_dir*/lib에서 수동으로 파일을 복사하십시오.
5. 그런 다음 Tivoli Access Manager for WebLogic을 구성하십시오. 23 페이지의 제 3 장 『구성 절차』로 이동하십시오

HP-UX에 설치

> **주의**
>
> HP-UX 플랫폼에 설치할 때 Tivoli Access Manager for WebLogic은 BEA WebLogic Server 버전 7.0에 대해서만 지원됩니다.

Tivoli Access Manager for WebLogic을 이미 설치 및 구성한 상태에서 다시 설치해야 할 경우, 우선 이를 구성 해제한 다음 제거해야 합니다. 51 페이지의 『HP-UX에서 제거』를 참조하십시오.

HP-UX에 Tivoli Access Manager for WebLogic을 설치하려면 다음 단계를 완료하십시오.

1. *root*로 로그인하십시오.
2. Tivoli Access Manager 기본의 필수 구성요소를 포함한 사전 설치 소프트웨어가 설치되어 있는지 확인하십시오. 12 페이지의 『사전 설치 소프트웨어』를 참조하십시오.
3. **pfs_mountd** 및 **pfsd**가 실행 중이지 않으면 백그라운드에서 이들을 차례대로 시작하십시오. **pfs_mount** 명령으로 CD를 마운트하십시오. 예를 들어, 다음 명령을 입력하십시오.

   ```
   /usr/sbin/pfs_mount /dev/dsk/c0t0d0 /cd-rom
   ```

   여기서 /dev/dsk/c0t0d0은 CD 디바이스이고 /cd-rom은 마운트 포인트입니다.
4. 다음 명령을 입력하여 Tivoli Access Manager for WebLogic 패키지를 설치하십시오.

   ```
   # swinstall -s /cd_rom/hp PDWLS
   ```

분석 단계가 완료되었음을 나타내는 메시지가 표시됩니다. 실행 단계가 시작됨을 나타내는 다른 메시지가 표시됩니다. 파일이 CD에서 추출되어 하드 디스크에 설치됩니다. 실행 단계가 완료되었음을 나타내는 메시지가 표시됩니다. **swinstall** 유틸리티가 종료됩니다.

주: 설치 프로그램이 AMSSPIProviders.jar 파일을 */bea_install_dir/*weblogic/server/lib/mbeantypes 디렉토리에 복사했는지 점검하십시오. 이 디렉토리에 해당 파일이 존재하지 않을 경우, */amwls_install_dir*/lib에서 수동으로 파일을 복사하십시오.

5. 그런 다음, Tivoli Access Manager for WebLogic을 구성하십시오. 23 페이지의 제 3 장 『구성 절차』로 이동하십시오

Solaris에 설치

Tivoli Access Manager for WebLogic을 설치하면 패키지 구성에서 파일이 추출됩니다. Solaris Operating Environment(이후 Solaris라고 함)에 소프트웨어 패키지를 설치하려면 **pkgadd**를 사용하십시오. 그런 다음, Tivoli Access Manager for WebLogic을 수동으로 구성하십시오

주: Tivoli Access Manager for WebLogic을 이미 설치 및 구성한 상태에서 다시 설치해야 할 경우, 우선 이를 구성 해제한 다음 제거해야 합니다. 49 페이지의 『Solaris에서 제거』를 참조하십시오.

Solaris에 Tivoli Access Manager for WebLogic을 설치하려면 다음 지시사항을 완료하십시오.

1. *root*로 로그인하십시오.
2. Tivoli Access Manager 기본의 필수 구성요소를 포함한 사전 설치 소프트웨어가 설치되어 있는지 확인하십시오. 12 페이지의 『사전 설치 소프트웨어』를 참조하십시오.
3. *Solaris용 IBM Tivoli Access Manager 웹 보안* CD를 넣으십시오.
4. 소프트웨어를 설치하려면 다음 명령을 실행하십시오.

   ```
   pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/solaris/pddefault PDWLS
   ```

   여기서,

-d /cdrom/cdrom0/solaris	패키지의 위치를 지정합니다.
-a /cdrom/cdrom0/solaris/pddefault	설치 관리 스크립트의 위치를 지정합니다.

각 패키지에 대해 설치 프로세스가 완료되면, 다음 메시지가 표시됩니다.

패키지 설치를 완료했습니다.

주: 설치 프로그램이 AMSSPIProviders.jar 파일을 */bea_install_dir/*weblogic/server/lib/mbeantypes 디렉토리에 복사했는지 점검하십시오. 이 디렉토리에 해당 파일이 존재하지 않을 경우, */amwls_install_dir*/lib에서 수동으로 파일을 복사하십시오.

5. 그런 다음, Tivoli Access Manager for WebLogic을 구성하십시오. 23 페이지의 제 3 장 『구성 절차』로 이동하십시오.

Windows에 설치

Tivoli Access Manager for WebLogic을 설치하면 패키지 구성에서 파일이 추출됩니다. Tivoli Access Manager for WebLogic 파일을 설치하려면 InstallShield **setup.exe**를 사용하십시오. InstallShield가 완료되면 23 페이지의 제 3 장 『구성 절차』의 지시사항을 사용하여 Tivoli Access Manager for WebLogic을 구성하십시오.

주: Tivoli Access Manager for WebLogic을 이미 설치 및 구성한 상태에서 다시 설치해야 할 경우, 우선 이를 구성 해제한 다음 제거해야 합니다. 50 페이지의 『Windows에서 제거』를 참조하십시오.

Windows에 Tivoli Access Manager for WebLogic을 설치하려면 다음 지시사항을 완료하십시오.

1. Administrator 권한이 있는 사용자로 Windows 도메인에 로그인하십시오.
2. Tivoli Access Manager 기본의 필수 구성요소를 포함한 사전 설치 소프트웨어가 설치되어 있는지 확인하십시오. 12 페이지의 『사전 설치 소프트웨어』를 참조하십시오.
3. *IBM Tivoli Access Manager Web Security for Windows* CD를 CD 드라이브에 넣으십시오.
4. 다음 파일을 두 번 눌러 Tivoli Access Manager for WebLogic InstallShield 설치 프로그램을 실행하십시오. 여기서 다음 명령에서 E:는 CD 드라이브를 표시합니다.

   ```
   E:\Windows\PolicyDirector\Disk Images\Disk1\PDWLS\Disk Images\Disk1\setup.exe
   ```

   설치 언어 선택 창이 열립니다.
5. 해당 언어를 선택한 후 **확인**을 누르십시오.

   InstallShield 프로그램이 시작되고 환영 창이 열립니다.
6. **다음**을 누르십시오.

   라이센스 계약 창이 열립니다.
7. 라이센스 계약을 읽은 후 계약 조건에 동의하면 **예**를 누르십시오.

   대상 위치 선택 창이 열립니다.
8. 기봉 위치를 채택하거나 다른 위치를 찾아보십시오. **다음**을 누르십시오.

파일 복사 시작 창이 열립니다.

9. 표시된 설치 위치가 올바른지 확인한 후 **다음**을 누르십시오.

   파일이 디스크로 추출됩니다. 파일이 설치되었음을 알리는 메시지가 표시됩니다.

10. **완료**를 눌러 설치 프로그램을 종료하십시오.
11. 설치 프로그램이 AMSSPIProviders.jar 파일을 c:*bea_install_dir*\weblogic\server\lib\mbeantypes 디렉토리에 복사했는지 점검하십시오. 이 디렉토리에 해당 파일이 존재하지 않을 경우, c:*amwls_install_dir*\lib에서 수동으로 파일을 복사하십시오.
12. 그런 다음, Tivoli Access Manager for WebLogic을 구성하십시오. 23 페이지의 제 3 장 『구성 절차』로 이동하십시오.

제 3 장 구성 절차

Tivoli Access Manager for WebLogic을 구성하려면 다음의 각각에 설명된 지시사항을 완료하십시오.

- 『제 1 부: Tivoli Access Manager Java Runtime Environment 구성』
- 25 페이지의 『제 2 부: startWebLogic에 대한 CLASSPATH 설정』
- 26 페이지의 『제 3 부: Tivoli Access Manager for WebLogic 구성』
- 29 페이지의 『제 4 부: Tivoli Access Manager 범위 구성』
- 32 페이지의 『제 5 부: BEA WebLogic Server 싱글 사인 온 구성』
- 34 페이지의 『제 6 부: 클러스터된 환경을 포함하여 BEA WebLogic Server 다중 서버 환경에서 Tivoli Access Manager for WebLogic 구성』
- 34 페이지의 『제 7 부: 구성 테스트』

주: 이 장에서는 Tivoli Access Manager 기본 구성요소의 구성을 포함하여 Tivoli Access Manager for WebLogic 및 사전 설치 소프트웨어를 설치한 것으로 가정합니다. 이 소프트웨어를 설치하지 않았으면 11 페이지의 제 2 장 『설치 지시사항』을 따라 지금 설치하십시오.

제 1 부: Tivoli Access Manager Java Runtime Environment 구성

Tivoli Access Manager Java Runtime Environment는 Tivoli Access Manager for WebLogic의 사전 설치 소프트웨어입니다. Java Runtime 구성요소를 올바르게 구성해야 BEA WebLogic Server 범위를 구성할 수 있습니다. Tivoli Access Manager 유틸리티 **pdjrtecfg**를 사용하여 BEA WebLogic Server에서 사용되는 JRE(Java Runtime Environment)를 갱신하십시오. 또한 시스템에 여러 Java 런타임이 포함된 경우, BEA WebLogic Server가 사용한 JRE(Java Runtime Environment)를 사용하여 **pdjrtecfg** 유틸리티를 실행하는지 확인하십시오.

1. Tivoli Access Manager 기본 JRE(Java Runtime Environment)가 설치되었는지 확인하십시오.

   자세한 정보는 12 페이지의 『사전 설치 소프트웨어』를 참조하십시오.

2. BEA WebLogic Server *WebLogic_install_dir*/server/bin 디렉토리에서 다음 스크립트를 실행하여 CLASSPATH 및 PATH 변수를 설정한 후 CLASSPATH, bin 및 lib 디렉토리에 WebLogic .jars를 추가하십시오.

   UNIX .setWLSEnv.sh

   Windows

   setWLSEnv.cmd

© Copyright IBM Corp. 2003

ezInstall을 실행하기 전에 BEA WebLogic Server와 함께 제공된 Java 실행 파일이 시스템 경로에서 맨 앞에 있는지 확인하십시오.

3. Tivoli Access Manager Java Runtime Environment는 BEA WebLogic Server와 함께 제공되고 설치된 JDK에 대해 구성되어야 합니다. 이를 수행하려면 다음과 같이 하십시오.

   a. Tivoli Access Manager 설치 경로에서 디렉토리를 sbin 디렉토리로 변경하십시오. 예를 들면, 다음과 같습니다.

      ```
      UNIX: /opt/PolicyDirector/sbin
      Windows: C:\Program Files\Tivoli\Policy Director\sbin
      ```

   b. 다음과 같이 **pdjrtecfg** 명령을 실행하십시오.

      ```
      pdjrtecfg -action config -host policy_server_name -java_home java_location
      ```

      여기서 *java_location*은 BEA WebLogic Server Java Runtime Environment의 디렉토리 위치입니다. 디렉토리의 위치는 다음과 같습니다.

      Windows

      BEA WebLogic Server 버전 7.0

      ```
      c:\bea\jdk131_ob\jre
      ```

      BEA WebLogic Server 버전 8.1

      ```
      c:\bea\jdk141\jre
      ```

      Solaris, HP-UX

      ```
      /usr/local/bea/jdk141_03
      ```

      AIX

      AIX 시스템에서 BEA WebLogic Server 7.0은 IBM Java Runtime Environment 버전 1.3이 필요하고 BEA WebLogic Server 8.1은 IBM Java Runtime Environment 버전 1.4가 필요합니다. **pdjrtecfg** 명령의 -java_home 옵션은 AIX 시스템에 있는 JRE의 설치 위치로 설정되어야 합니다. BEA WebLogic Server 버전 7.0

      ```
      /usr/java131
      ```

      BEA WebLogic Server 버전 8.1

      ```
      /usr/java14
      ```

      주:

      1) BEA WebLogic Server 8.1 설치의 **pdjrtecfg** 유틸리티는 jre/lib 디렉토리의 jsse.jar을 바꿉니다. 이 파일은 Tivoli Access Manager Java Runtime이 구성 해제될 때 다시 원상태로 됩니다.

      2) Sun v1.4d JRE를 구성할 때, 구성이 실패하므로 **pdjrtecfg**를 대화식 모드로 실행하거나 **pdconfig** 유틸리티를 사용하여 JRE를 구성하지 마십시오.

pdjrtecfg 사용에 대한 자세한 정보는 *IBM Tivoli Access Manager 기본 설치 안내서*를 참조하십시오.

제 2 부: startWebLogic에 대한 CLASSPATH 설정

주: 이들 구성 단계를 실행하기 전에 WebLogic 도메인을 작성했는지 확인하십시오.

startWebLogic 명령을 사용하여 WebLogic 서버를 시작합니다. **startWebLogic**을 사용하여 올바른 Java 클래스에 액세스하고 로드할 수 있도록 CLASSPATH 환경 변수를 수정해야 합니다.

다음 지시사항을 완료하십시오.

1. WebLogic 서버가 실행 중인 경우 중지하십시오.
2. **startWebLogic** 명령의 CLASSPATH 변수에 다음 파일 이름을 추가하십시오.

   UNIX

   ```
   /opt/pdwls/lib/AMSSPICore.jar
   /opt/pdwls/lib/rbpf.jar
   ```

   Windows

   ```
   C:\amwls_install_directory\lib\AMSSPICore.jar
   C:\amwls_install_directory\lib\rbpf.jar
   ```

   startWebLogic 명령은 BEA WebLogic Server 설치 도메인의 디렉토리에 있습니다. 표준 설치의 경우 다음과 같습니다.

   UNIX */WebLogic_install_directory*/user_projects/*domain_name*

   Windows

   ```
   C:\WebLogic_install_directory\user_projects\domain_name
   ```

   변수 *domain_name*은 BEA WebLogic Server 도메인을 작성할 때 선택한 이름입니다.
3. 기본 언어(영어)를 사용하는 경우 이 단계를 건너뛰십시오.

   언어 팩을 사용하여 영어(기본값) 이외의 언어를 지원할 경우, 다음 경로를 **startWebLogic** 스크립트에 정의된 CLASSPATH에 추가해야 합니다.

   UNIX

   ```
   /opt/pdwls/nls/java/com/tivoli/amwls/sspi/nls
   ```

   Windows

   ```
   C:\Progra~1\Tivoli\pdwls\nls\java\com\tivoli\amwls\sspi\nls
   ```

   주: 이 디렉토리를 추가하면, 언어 팩 설치 시 /opt/pdwls/nls/java/com/tivoli/amwls/sspi/nls/에 설치된 자원 번들에 액세스할 수 있습니다.

제 3 부: Tivoli Access Manager for WebLogic 구성

Tivoli Access Manager for WebLogic은 명령행을 사용하여 구성하거나 Tivoli Access Manager Console Extension Web Application을 사용하여 구성할 수 있습니다. 이들 두 가지 옵션에 대한 세부사항은 아래의 절에서 설명됩니다.

BEA WebLogic Server 도메인은 이러한 지시사항을 실행하기 전에 작성되어야 합니다.

Tivoli Access Manager for WebLogic을 구성하고 범위를 작성할 때 입력되는 데이터는 특성 파일에 저장됩니다. 이들 특성 파일은 Tivoli Access Manager for WebLogic의 작동을 변경하는 데 사용할 수 있습니다. 자세한 정보는 53 페이지의 부록 A『특성 파일 참조』를 참조하십시오.

Console Extension Web Application을 사용하여 Tivoli Access Manager for WebLogic 구성

1. BEA WebLogic Server를 시작하십시오.

   UNIX */WLS_install_dir*/user_projects/*domain_name*/startWebLogic.sh

   Windows

   C:*WLS_install_dir*\user_projects*domain_name*\
   startWebLogic.cmd

2. BEA WebLogic을 호스트하는 시스템에서 웹 브라우저를 열고 BEA WebLogic 콘솔에 연결하십시오. 즉, 다음과 같이 연결 하십시오.

   http://*WebLogic_server_name*:7001/console

   7001은 기본 BEA WebLogic Server 포트 번호입니다. 이 값은 구성 가능합니다.

3. BEA WebLogic Server 로그온 화면이 표시됩니다. 관리자 권한이 있는 BEA WebLogic Server 사용자로 로그온하십시오.

4. Tivoli Access Manager for WebLogic Server를 구성하고 Tivoli Access Manager 범위를 작성하기 전에 먼저 구성 태스크에 대한 웹 인터페이스를 제공하는 Tivoli Access Manager Console Extension Web Application을 배치해야 합니다. 이 웹 어플리케이션을 배치하려면 다음을 수행 하십시오.

   a. BEA WebLogic Server 홈 페이지의 *도메인 구성* 배너 내에서 *웹 어플리케이션*을 선택하십시오.

   b. **새 웹 어플리케이션 구성** 링크를 선택하십시오.

   c. **브라우저를 통해 업로드** 링크를 선택하십시오.

   d. 어플리케이션 *amwls_install_dir*\lib\AMWLSConsoleExtension.war을 찾아보십시오. **업로드**를 누르십시오.

   e. AMWLSConsoleExtension.war에 대한 **선택** 링크를 누르십시오.

f. 배치 대상을 선택한 후 **구성 및 표시**를 누르십시오.

Console Extension Web Application이 성공적으로 배치되었는지 점검하려면 왼쪽 화면 분할창의 *배치* 폴더를 펼치십시오. *웹 어플리케이션* 폴더를 펼치십시오. *AMWLSConsoleExtensions*가 목록에 표시되어야 합니다. 또한 콘솔 웹 어플리케이션 확장을 전개하면 콘솔 창의 왼쪽에 표시된 BEA WebLogic Server 탐색 분할창에 Tivoli Access Manager 아이콘을 추가합니다.

5. Tivoli Access Manager 도메인을 구성하려면 BEA WebLogic Server 탐색 분할창의 *Access Manager* 아이콘을 누르십시오.
6. 구성 화면이 표시됩니다. 모든 필수 정보 및 선택적 매개변수를 입력하십시오. 입력할 정보에 대한 지시사항은 아래의 표를 참조하십시오.

`config` 조치에 사용 가능한 옵션이 아래의 표에 나열됩니다. 첫 번째 표에는 *필수* 옵션이 나열됩니다. 두 번째 표에는 *선택적* 옵션이 나열됩니다.

필수 옵션 이름	설명
domain_admin	WebLogic 도메인 관리자
domain_admin_pwd	WebLogic 도메인 관리자 암호
remote_acl_user	Authorization Server용으로 작성되는 Tivoli Access Manager 프린시펄(사용자)
sec_master_pass	Tivoli Access Manager sec_master 관리자 암호
pdmgrd_host	Tivoli Access Manager Policy Server 호스트 이름
pdacld_host	Tivoli Access Manager Authorization Server 호스트 이름

주: 암호는 입력할 필요가 없으며 대신 조치가 수행되기 전에 프롬프트로 표시됩니다. 이렇게 하면 암호가 명령 히스토리에 남게 되지 않습니다.

다음 표에는 `config` 조치에 대한 *선택적* 옵션이 나열됩니다.

옵션 이름	설명
wls_server_url	로컬 WebLogic 서버에 대한 URL을 지정합니다. 기본값은 `t3://localhost:7001`입니다.
pdmgrd_port	Tivoli Access Manager Policy Server 포트 번호
pdacld_port	Tivoli Access Manager Authorization Server 포트 번호
am_domain	Tivoli Access Manager 도메인의 이름을 지정합니다. 기본값은 `Default`입니다.
amwls_home	Tivoli Access Manager for WebLogic Server 설치 디렉토리에 대한 경로를 지정합니다.

적용을 누르십시오.

7. 구성이 완료되면, Tivoli Access Manager for WebLogic Server 매개변수 목록이 오른쪽 분할창에 표시됩니다.

이제 Tivoli Access Manager 범위를 구성할 수 있습니다. 29 페이지의 『제 4 부: Tivoli Access Manager 범위 구성』을 참조하십시오.

명령행에서 Tivoli Access Manager for WebLogic 구성

1. BEA WebLogic Server를 시작하십시오.

   UNIX

   /WLS_install_dir/user_projects/*domain_name*/startWebLogic.sh

   Windows

   C:*WLS_install_dir*\user_projects*domain_name*\startWebLogic.cmd

2. Tivoli Access Manager for WebLogic을 구성하려면 다음 명령을 실행하십시오.

   주: 파일 추출 중 Tivoli Access Manager for WebLogic이 권장된 위치에 설치되지 않은 경우(이전 장에서 설명한 대로), **AMWLSConfigure** 스크립트의 AMSSPI_DIR 변수를 반드시 실제 설치 디렉토리의 위치로 설정하십시오. 마찬가지로, WebLogic이 기본 위치에 설치되지 않았으면, WLS_JAR 변수를 **ALWLSConfigure** 스크립트에 있는 WebLogic.jar의 올바른 위치로 갱신하십시오.

   UNIX *install-dir*/sbin/AMWLSConfigure.sh

   Windows

   install-dir\sbin\AMWLSConfigure.bat

   Tivoli Access Manager for WebLogic을 구성하기 위한 **AMWLSConfigure** Java 어플리케이션에 대한 명령행 구문은 다음과 같습니다.

   - AMWLSConfigure -action config [*options* ...]

     Tivoli Access Manager for WebLogic을 구성합니다.

   - AMWLSConfigure -help [*action*]

     AMSSPIConfigure로 전달하기 위한 필수 및 선택적 값을 표시합니다.

   config 조치에 사용 가능한 옵션이 아래의 표에 나열됩니다. 첫 번째 표에는 *필수* 옵션이 나열됩니다. 두 번째 표에는 *선택적* 옵션이 나열됩니다.

필수 옵션 이름	설명
domain_admin	WebLogic 도메인 관리자
domain_admin_pwd	WebLogic 도메인 관리자 암호
remote_acl_user	Authorization Server용으로 작성되는 Tivoli Access Manager 프린시펄(사용자)
sec_master_pass	Tivoli Access Manager sec_master 관리자 암호
pdmgrd_host	Tivoli Access Manager Policy Server 호스트 이름
pdacld_host	Tivoli Access Manager Authorization Server 호스트 이름

   주: 암호는 입력할 필요가 없으며 대신 조치가 수행되기 전에 프롬프트로 표시됩니다. 이렇게 하면 암호가 명령 히스토리에 남게 되지 않습니다.

다음 표에는 config 조치에 대한 *선택적* 옵션이 나열됩니다.

옵션 이름	설명
deploy_extension	true로 설정할 경우, Tivoli Access Manager for Web Logic Server 콘솔 확장을 배치합니다. 기본값은 true입니다.
wls_server_url	로컬 WebLogic 서버에 대한 URL을 지정합니다. 기본값은 t3://localhost:7001입니다.
pdmgrd_port	Tivoli Access Manager Policy Server 포트 번호
pdacld_port	Tivoli Access Manager Authorization Server 포트 번호
am_domain	Tivoli Access Manager 도메인의 이름을 지정합니다. 기본값은 Default입니다.
amwls_home	Tivoli Access Manager for WebLogic Server 설치 디렉토리에 대한 경로를 지정합니다.
verbose	자세한 출력을 사용 가능 또는 사용 불가능하게 하는 부울 값. 기본값은 false입니다.

이제 Tivoli Access Manager 범위를 구성해야 합니다.

제 4 부: Tivoli Access Manager 범위 구성

Console Extension Web Application을 사용하여 Tivoli Access Manager 범위 구성

Tivoli Access Manager for WebLogic Server를 BEA WebLogic Server의 보안을 제공하도록 구성한 후에는 Tivoli Access Manager 보안과 연관시킬 범위를 작성해야 합니다. 이를 수행하려면 다음과 같이 하십시오.

1. 왼쪽 화면 분할창의 *Access Manager* 아이콘을 펼친 후 *범위* 아이콘을 누르십시오.
2. *범위 작성* 화면이 표시됩니다. 모든 필수 변수를 입력하십시오. 적용을 누르십시오.
3. BEA WebLogic Server 7.0을 위에서 작성한 Tivoli Access Manager 범위를 사용하도록 구성하려면, 다음을 수행하십시오.
   a. BEA WebLogic Server 탐색 분할창에서 사용자의 도메인과 관련된 아이콘을 선택하십시오.
   b. *도메인 구성* 화면이 표시됩니다. *보안* 탭을 선택하십시오.
   c. *일반* 탭에서 *기본 범위* 드롭 다운 목록을 사용하여 위의 단계에서 작성한 범위를 선택하십시오. *적용*을 누르십시오.

   BEA WebLogic Server 8.1을 위에서 작성한 Tivoli Access Manager 범위를 사용하도록 구성하려면 BEA WebLogic Server 콘솔의 보안 탭을 사용하여 기본 범위를 설정하십시오.
4. BEA WebLogic Server를 다시 시작하십시오.

5. 새 Access Manager 범위가 올바로 기능하는지 테스트하려면, 오른쪽 화면 분할창의 *Access Manager* 폴더 내에 있는 *사용자* 및 *그룹* 아이콘에 Tivoli Access Manager 사용자 레지스트리의 항목이 포함되어 있어야 합니다.

주: 이미 존재하는 SSO 사용자를 지정했지만 기존 사용자에 대해 정확하지 않은 암호를 입력한 경우, 범위 작성 조치가 완료되기는 하지만 SSO는 표시되지 않습니다. 이러한 경우, Tivoli Access Manager for WebLogic `rbpf.properties` 파일에서 적절한 항목을 갱신하여 SSO를 쉽게 사용 가능하게 할 수 있습니다. `rbpf.properties`에 대한 자세한 내용은 53 페이지의 부록 A『특성 파일 참조』를 참조하십시오.

명령행에서 Tivoli Access Manager 범위 구성

1. Tivoli Access Manager for WebLogic 범위를 작성하려면 다음 명령을 실행하십시오.

   주: 파일 추출 중 Tivoli Access Manager for WebLogic이 권장된 위치에 설치되지 않은 경우(이전 장에서 설명한 대로), **AMWLSConfigure** 스크립트의 `AMSSPI_DIR` 변수를 반드시 실제 설치 디렉토리의 위치로 설정하십시오. 마찬가지로 WebLogic이 기본 위치에 설치되지 않았거나 WebLogic 버전 8.1을 사용 중인 경우, `WLS_JAR` 변수를 **ALWLSConfigure** 스크립트에 있는 `WebLogic.jar`의 올바른 위치로 갱신하십시오.

   UNIX *install-dir*`/sbin/AMWLSConfigure.sh`

   Windows

   install-dir`\sbin\AMWLSConfigure.bat`

   Tivoli Access Manager for WebLogic을 구성하기 위한 **AMWLSConfigure** Java 어플리케이션에 대한 명령행 구문은 다음과 같습니다.

   - `AMWLSConfigure -action create_realm [`*options* `...]`

     Tivoli Access Manager for WebLogic 범위를 작성합니다.

   - `AMWLSConfigure -help [`*action*`]`

     AMSSPIConfigure로 전달하기 위한 필수 및 선택적 값을 표시합니다.

   `create_realm` 조치에 사용 가능한 옵션이 아래의 표에 나열됩니다. 첫 번째 표에는 *필수* 옵션이 나열됩니다. 두 번째 표에는 *선택적* 옵션이 나열됩니다.

필수 옵션 이름	설명
realm_name	작성되고 있는 WLS 범위의 이름을 지정합니다.
domain_admin_pwd	WebLogic 도메인 관리자 암호를 지정합니다.
user_dn_suffix	Console Extension Web Application을 통해 사용자를 작성할 때 사용할 구별 이름(DN) 접미어를 지정합니다.

group_dn_suffix	Console Extension Web Application을 통해 그룹을 작성할 때 사용할 구별 이름(DN) 접미어를 지정합니다.
admin_group	내부 구성 용도에 사용할 Tivoli Access Manager 그룹을 지정합니다.

주: 암호는 입력할 필요가 없으며 대신 조치가 수행되기 전에 프롬프트로 표시됩니다. 이렇게 하면 암호가 명령 히스토리에 남게 되지 않습니다.

다음 표에는 `create_realm` 조치에 대한 *선택적* 옵션이 나열됩니다.

옵션 이름	설명
user_dn_prefix	Console Extension Web Application을 통해 사용자를 작성할 때 사용할 구별 이름(DN) 접두어를 지정합니다.
group_dn_prefix	Console Extension Web Application을 통해 그룹을 작성할 때 사용할 구별 이름(DN) 접두어를 지정합니다.
sso_enabled	true로 설정할 경우 싱글 사인 온 지원을 사용 가능하게 합니다. 기본값은 `false`입니다.
sso_user	Tivoli Access Manager와 싱글 사인 온 신뢰 연관을 작성하기 위한 사용자를 지정합니다.
sso_pwd	싱글 사인 온 사용자에 대한 암호를 지정합니다.
verbose	자세한 출력을 사용 가능 또는 사용 불가능하게 하는 부울 값. 기본값은 `false`입니다.

2. BEA WebLogic Server 7.0을 위에서 작성한 Tivoli Access Manager 범위를 사용하도록 구성하려면, 다음을 수행하십시오.
   a. BEA WebLogic을 호스트하는 시스템에서 웹 브라우저를 열고 BEA WebLogic 콘솔에 연결하십시오. 즉, 다음과 같이 하십시오.

      `http://`*`WebLogic_server_name`*`:7001/console`

      7001은 기본 BEA WebLogic Server 포트 번호이며, 이 값은 구성 가능합니다.
   b. BEA WebLogic Server 로그온 화면이 표시됩니다. 관리자 권한이 있는 사용자로 로그온하십시오.
   c. BEA WebLogic Server 탐색 분할창에서 사용자의 도메인과 관련된 아이콘을 선택하십시오.
   d. *도메인 구성* 화면이 표시됩니다. *보안* 탭을 선택하십시오.
   e. *일반* 탭에서 *기본 범위* 드롭 다운 목록을 사용하여 위의 단계에서 작성한 범위를 선택하십시오. *적용*을 누르십시오.

   BEA WebLogic Server 8.1을 위에서 작성한 Tivoli Access Manager 범위를 사용하도록 구성하려면 BEA WebLogic Server 콘솔의 보안 탭을 사용하여 기본 도메인을 설정하십시오.
3. BEA WebLogic Server를 다시 시작하십시오.

4. 새 Access manager 범위가 올바로 기능하는지 테스트하려면 왼쪽 분할 창의 *Access Manager* 폴더 내에 있는 *사용자* 및 *그룹* 아이콘에 Tivoli Access manager 사용자 레지스트리의 항목이 포함되어 있어야 합니다.

제 5 부: BEA WebLogic Server 싱글 사인 온 구성

이 절에서는 WebSEAL 또는 Tivoli Access Manager Plug-in for Web Servers를 사용하여 BEA WebLogic Server에 대한 싱글 사인 온을 구성하는 프로세스에 대해 설명합니다. 싱글 사인 온 구성을 구현하지 않으려는 경우 이 절을 무시할 수 있습니다.

WebSEAL 및 Tivoli Access Manager Plug-in for Web Servers는 보안 및 싱글 사인 온을 서로 다른 방법으로 구현하고 서로 다른 시스템 구조를 사용합니다. WebSEAL 및 웹 서버에 대한 플러그인을 설치하는 데 대한 정보는 *IBM Tivoli Access Manager for e-business Web Security Installation Guide*를 참조하십시오. WebSEAL 구성에 대한 백그라운드 정보 및 자세한 내용은 *IBM Tivoli Access Manager for e-business WebSEAL Administration Guide*를 참조하십시오. 플러그인에 대한 운영 및 구성 정보에 대해서는 *IBM Tivoli Access Manager Plug-in for Web Servers Integration Guide*를 참조하십시오.

다음 절에서는 구현하려는 구조에 따라 BEA WebLogic Server에 대한 싱글 사인 온을 구성하는 데 필요한 추가 WebSEAL 및 플러그인 구성 정보를 제공합니다.

- 『WebSEAL 정션을 사용하여 싱글 사인 온 구성』
- 33 페이지의 『Tivoli Access Manager Plug-in for Web Servers를 사용하여 싱글 사인 온 구성』

WebSEAL 정션을 사용하여 싱글 사인 온 구성

WebSEAL을 사용하여 BEA WebLogic Server의 싱글 사인 온 기능을 제공하려면 WebSEAL 서버를 호스트하는 시스템에서 다음 단계를 완료하십시오.

1. WebSEAL 구성 파일 `webseald.conf`를 여십시오.
2. 다음 구성 항목을 설정하십시오.

   ```
   basicauth-dummy-passwd = sso_pwd
   ```

   이 암호는 범위 작성 조치 중 사용 가능하게 된 `sso_pwd` 필드의 암호와 일치해야 합니다.
3. WebSEAL을 중지한 후 다시 시작하여 구성 변경사항을 적용하십시오.
4. **pdadmin** 명령을 사용하여 WebSEAL 정션을 작성하십시오.

주: Tivoli Access Manager 보안 도메인에 있는 모든 시스템에서 이 단계를 수행할 수 있습니다. WebSEAL 시스템에서는 이를 실행할 필요가 없습니다. 예를 들어, Tivoli Access Manager Policy Server 시스템에서 이를 실행할 수 있습니다.

`-b` 옵션을 사용하여 junction 대상 URL을 제공해야 합니다. 이는 싱글 사인 온에 필수입니다.

예를 들어, 다음 명령을 *한 명령행에 연속해서* 입력하십시오.

```
pdadmin> server task webseald_server_name create -t tcp
-p WebLogic_Server_listen_port -h WebLogic_Server
-b supply junction_target
```

다음 표에서는 위 **pdadmin** 명령의 변수를 정의합니다.

표 2. pdadmin 명령에 대한 옵션

옵션	설명
webseald_server_name	WebSEAL 서버의 이름. 이 이름은 두 부분(예: `webseald-`*WebSEAL_server_instance*)으로 이루어집니다. *WebSEAL_server_instance*에는 시스템의 호스트 이름을 사용하십시오. 예를 들어, 호스트 시스템 이름이 `cruz`인 경우 *webseald_server_name*은 `webseald-cruz`입니다. 주: 여러 개의 WebSEAL 인스턴스를 동일한 서버에 설치한 경우, 해당 서버 인스턴스도 지정해야 합니다. 다중 서버 인스턴스를 사용하여 junction을 작성하는 데 대한 지시사항은 *IBM Tivoli Access Manager for e-business WebSEAL Administration Guide*를 참조하십시오.
WebLogic_Server	BEA WebLogic Server의 호스트 이름
WebLogic_Server_listen_port	BEA WebLogic Server가 인식하고 있는 포트. 기본값은 7001입니다.
-b supply	싱글 사인 온에 필요합니다. WebSEAL이 더미 암호를 전달하도록 하십시오.
junction_target	junction의 URL 대상

WebSEAL junction 작성 및 사용에 대한 전체 정보는 *IBM Tivoli Access Manager for e-business WebSEAL Administration Guide*를 참조하십시오.

Tivoli Access Manager Plug-in for Web Servers를 사용하여 싱글 사인 온 구성

싱글 사인 온이 올바로 작업하게 하려면 Tivoli Access Manager Plug-in for Web Servers가 기본 인증 헤더에 있는 올바른 정보를 IBM Tivoli Access Manager for WebLogic Server로 전달하도록 구성해야 합니다. 이렇게 하려면, 기본 인증을 플러그인 구성 파일의 사후 권한 모듈로 구성해야 합니다.

plug-in_install_dir`/etc` 디렉토리에 위치한 `pdwebpi.conf` 구성 파일을 편집하여 **[common-modules]** 스탠자에 다음 값을 추가하십시오.

```
[common-modules]
post-authzn = BA
```

그런 다음, **[BA}** 스탠자에 있는 **add-hdr** 및 **supply-password** 매개변수를 각각 *BA* 및 sso_user의 암호로 설정하십시오. 즉, 다음과 같이 하십시오.

```
[BA]
add-hdr = supply
supply-password = sso_pwd
```

Tivoli Access Manager Plug-in for Web Servers 구성에 대한 자세한 정보는 *IBM Tivoli Plug-in for Web Servers Integration Guide*를 참조하십시오.

제 6 부: 클러스터된 환경을 포함하여 BEA WebLogic Server 다중 서버 환경에서 Tivoli Access Manager for WebLogic 구성

이 절은 BEA WebLogic Server가 다중 서버 환경 또는 클러스터된 환경으로 설정되어 있는 구조에 대한 경우입니다. 클러스터된 환경을 포함하여 BEA WebLogic Server 다중 서버 환경에서 Tivoli Access Manager for WebLogic을 구성하려면, 다음을 수행하십시오.

1. 26 페이지의 『제 3 부: Tivoli Access Manager for WebLogic 구성』 및 29 페이지의 『제 4 부: Tivoli Access Manager 범위 구성』의 지시사항을 사용하여 Tivoli Access Manager for WebLogic을 구성하고 BEA WebLogic Server 관리 서버에서 Tivoli Access Manager 범위를 작성하십시오.
2. 도메인에 대한 관리 서버의 Tivoli Access Manager for WebLogic 특성을 각 대상 시스템(관리 서버)에 복사하여 클러스터 구성원을 포함한 관리 서버의 Tivoli Access Manager for WebLogic을 사용 가능하게 하십시오. 특성 파일은 BEA_WLS_HOME/jdk_location/jre/amwls/에 위치하며 각 관리 서버의 동일한 위치에 복사되어야 합니다.

제 7 부: 구성 테스트

다음 단계를 완료하여 Tivoli Access Manager for WebLogic이 Tivoli Access Manager 레지스트리에 대해 올바로 구성되었는지 검증하십시오.

1. BEA WebLogic Server 콘솔을 사용하여 새 테스트 사용자를 작성하고 유효성을 검증하십시오.
2. 다음 **pdadmin** 명령을 실행하십시오.

   ```
   pdadmin> user show test_user
   ```

   - account-valid가 yes인지 확인하십시오.
   - password-valid가 yes인지 확인하십시오.

Tivoli Access Manager for WebLogic 싱글 사인 온 솔루션을 사용하면 BEA WebLogic Server에 대해 사용자를 투명하게 인증하는 WebSEAL을 통해 싱글 인증 단계를 수행할 수 있습니다. 데모 어플리케이션을 실행하여 인증이 올바로 구성되었는지 확인할 수 있습니다. 데모 어플리케이션은 41 페이지의 『데모 어플리케이션 사용』에 설명되어 있습니다.

제 4 장 싱글 사인 온 사용 가능

Tivoli Access Manager WebSEAL을 사용한 싱글 사인 온

Tivoli Access Manager for WebLogic은 기타 Tivoli Access Manager 제품(예: Tivoli Access Manager WebSEAL, Tivoli Access Manager Plug-in for Web Servers 및 Tivoli Access Manager Plug-in for Edge Server)에서의 웹 싱글 사인 온을 지원합니다.

WebSEAL과 BEA WebLogic Server 간의 신뢰 관계는 구성된 HTTP 기본 인증 *dummy* 암호를 사용하여 이루어집니다. 사용자 정의 보안 범위 인터페이스를 구현하는 이전의 Tivoli Access Manager for BEA WebLogic Server 제품에서는 싱글 사인 온을 수행하기 위해 이러한 동일한 방법을 사용했습니다.

Tivoli Access Manager HTTP 역프록시(예: WebSEAL)는 사용자 이름 및 알려진 싱글 사인 온 비밀 암호를 전달하도록 구성됩니다. 이 비밀 암호는 역프록시가 *신뢰성이 있는지* 판별하는 데 사용됩니다. Tivoli Access Manager Authorization Server가 암호를 검증한 후, 자원을 요청하는 사용자에 대한 권한 정보가 확보됩니다.

아래의 그림에서는 신뢰 관계가 확립되는 방법을 자세히 보여줍니다.

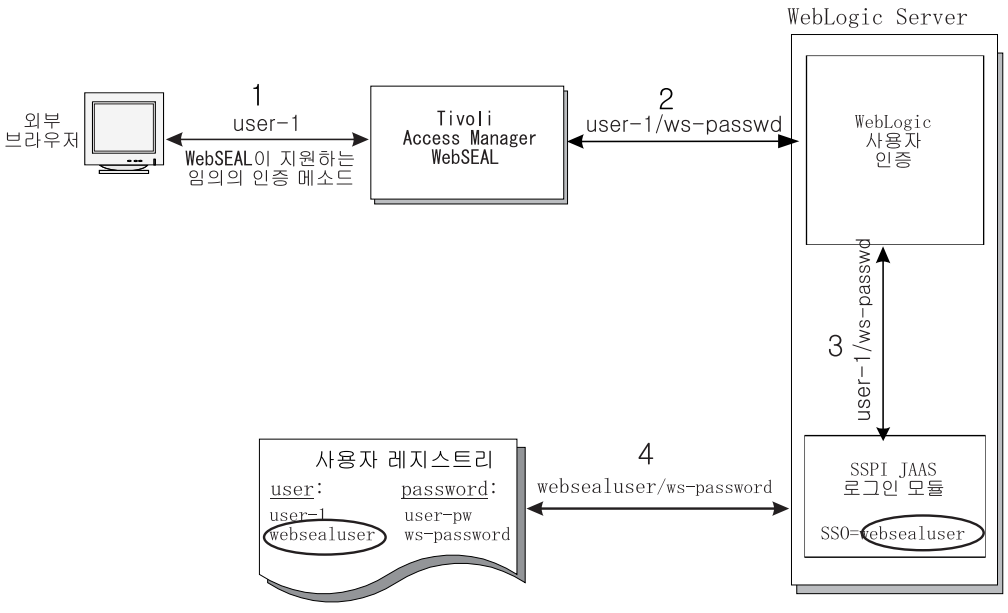

그림 3. Tivoli Access Manager WebSEAL을 사용한 싱글 사인 온

위의 그림에서는 다음 단계를 보여줍니다.

© Copyright IBM Corp. 2003

1. 사용자는 WebSEAL이 지원하는 인증 메커니즘(예: 사용자 이름/암호 또는 클라이언트 인증)을 사용하여 WebSEAL에 대해 인증합니다. 그런 다음, 사용자는 BEA WebLogic Server 자원에 대한 요청을 제출합니다.
2. WebSEAL은 `-b supply` 옵션을 사용하여 BEA WebLogic Server에 대한 정션으로 구성됩니다. WebSEAL은 다음을 포함하는 기본 인증 헤더를 사용하여 BEA WebLogic Server로 요청을 전달합니다.
   - WebSEAL 인증 사용자 ID(다이어그램에서 **user-1**)
   - `webseald.conf`의 `basicauth-dummy-passwd`. 이는 위에서 언급된 비밀 암호입니다.
3. BEA WebLogic Server는 검증을 위해 Tivoli Access Manager for WebLogic 인증 제공자에게 사용자 ID 및 비밀 암호를 전달합니다.
4. Tivoli Access Manager for WebLogic 로그인 모듈은 Tivoli Access Manager를 사용하여 제공된 암호가 Tivoli Access Manager for WebLogic 구성 WebSEAL 싱글 사인 온 사용자에 대한 것인지 검증합니다. 이 암호의 검증은 WebSEAL과 BEA WebLogic Server 간에 신뢰 관계를 제공합니다.

   4단계를 완료하면, Tivoli Access Manager for WebLogic 인증 제공자는 BEA WebLogic Server에 대해 제공된 사용자 ID를 인증합니다. 비밀 암호(다이어그램에서 `ws-passwd`)를 사용하는 구성된 WebSEAL 싱글 사인 온 사용자의 인증은 Tivoli Access Manager for WebLogic 로그인 모듈에 캐시되기 때문에 한번만 수행되는 점을 주지하십시오. 이 캐시는 구성할 수 있으며 꺼짐으로 설정할 수 있습니다.

SSO는 범위 작성 중 설정할 수 있지만 SSO Tivoli Access Manager for WebLogic를 수동으로 사용 가능하게 하려면 다음을 수행 하십시오.

1. SSO 사용자를 작성하십시오.
2. `amsspi.properties` Tivoli Access Manager for WebLogic 구성 파일에서 다음을 설정하십시오.

```
com.tivoli.amwls.sspi.Authentication.ssoEnabled = true
com.tivoli.amwls.sspi.Authentication.ssoTrustId = sso_username
```

제 5 장 관리 태스크

이 장은 Tivoli Access Manager for WebLogic에 대한 다음 정보로 구성되어 있습니다.

- 『Tivoli Access Manager Authorization Server에서 인타이틀먼트 서비스 사용』
- 40 페이지의 『Tivoli Access Manager for WebLogic에서 사용자 및 그룹 관리』
- 41 페이지의 『데모 어플리케이션 사용』
- 43 페이지의 『사용 팁』
- 44 페이지의 『3회 시도 로그온 policy』
- 45 페이지의 『Tivoli Access Manager 범위 삭제』
- 46 페이지의 『Tivoli Access Manager for WebLogic 구성 해제』
- 46 페이지의 『문제점 해결 팁』
- 47 페이지의 『제한사항』

Tivoli Access Manager Authorization Server에서 인타이틀먼트 서비스 사용

Tivoli Access Manager for WebLogic은 Tivoli Access Manager 보호 오브젝트 데이터베이스에서 보호 오브젝트를 찾아보려면 기본적으로 Tivoli Access Manager Policy Server를 사용합니다. 그러나, 이 구조는 Tivoli Access Manager Policy Server를 복제할 수 없으며 Tivoli Access Manager for WebLogic 단일 실패 지점을 소개하므로 테스트 환경에서만 사용되어야 합니다. 그 밖에, 인타이틀먼트 서비스는 내부 캐싱 기술에 따라 더 큰 런타임 성능을 가집니다. **인타이틀먼트 서비스 구조는 항상 프로덕션 환경에서 사용되어야 합니다.**

다음 구성 단계는 Tivoli Access Manager for WebLogic이 올바로 구성된 후에만 수행됩니다. Tivoli Access Manager for WebLogic은 두 개의 인타이틀먼트 서비스를 사용하며 이들 서비스는 둘다 구성된 모든 Tivoli Access Manager Authorization Server에서 사용 가능하게 되어야 합니다.

- **Tivoli Access Manager 확장 속성 인타이틀먼트 서비스**
  이는 Tivoli Access Manager Authorization Server를 사용하여 분배된 기본 인타이틀먼트 서비스입니다.
- **RBPF 보호 오브젝트 찾아보기 인타이틀먼트 서비스**
  이는 Tivoli Access Manager for WebLogic을 사용하여 분배된 인타이틀먼트 서비스입니다.

© Copyright IBM Corp. 2003

Tivoli Access Manager for WebLogic이 인타이틀먼트 서비스를 사용 중인지 확인하려면 다음 단계를 수행하십시오.

1. Tivoli Access Manager for WebLogic 호스트에서 Tivoli Access Manager Authorization Server 호스트로 **rbpf_ent_pos_browser** 공유 라이브러리를 복사한 후, 시스템 PATH에 위치한 임의의 디렉토리에 넣으십시오.
   rbpf_ent_pos_browser 공유 라이브러리는 다음의 Tivoli Access Manager for WebLogic 호스트에서 찾을 수 있습니다.

   UNIX `/opt/PolicyDirector/lib`

   Windows

   ```
   c:\Program Files\Tivoli\pdwls\bin
   ```

2. Tivoli Access Manager Authorization 호스트에서 다음 위치에 있는 `ivacld.conf` 파일을 여십시오.

   UNIX `/opt/PolicyDirector/etc`

   Windows

   ```
   c:\Program Files\Tivoli\Policy Director\etc
   ```

3. **[aznapi-entitlement-services]** 스탠자에 다음 두 라인을 추가하십시오.

   ```
   AZN_ENT_EXT_ATTR = azn_ent_ext_attr
   RBPF_POS_BROWSE = rbpf_ent_pos_browser
   ```

4. Tivoli Access Manager Authorization Server를 다시 시작하십시오.
5. Tivoli Access Manager for WebLogic 호스트에서 *java_home*`/amwls/WLS_Domain_Name/WLS_Realm_Name`에 위치한 `rbpf.properties` 파일을 여십시오. 여기서, *WLS_Domain_Name*은 BEA WebLogic Server 도메인의 이름이고 *WLS_Realm_Name*은 BEA WebLogic Server 보안 범위의 이름입니다. 다음 특성을 *true*로 갱신하십시오.

   ```
   com.tivoli.pd.as.rbpf.UseEntitlements=true
   ```

6. BEA WebLogic Server를 다시 시작하십시오.

이들 단계가 완료되면, Tivoli Access Manager for WebLogic 사용 가능 BEA WebLogic Server는 Tivoli Access Manager Policy Server와 반대로 Tivoli Access Manager Authorization Server를 사용하여 모든 보호 오브젝트 찾아보기를 수행합니다.

Tivoli Access Manager for WebLogic에서 사용자 및 그룹 관리

Tivoli Access Manager for WebLogic에서 BEA WebLogic Server 콘솔을 사용하여 사용자 및 그룹을 관리할 수 있습니다. BEA WebLogic Server 콘솔의 보안 분할창에서 *Access Manager* 아이콘을 펼친 후 *범위* 아이콘을 눌러 **사용자** 및 **그룹** 아이콘을 표시하십시오. 이들 아이콘에서 Tivoli Access Manager for WebLogic 보안에 대한 사용자 및 그룹을 관리할 수 있습니다.

사용자 아이콘을 선택하면 *사용자 관리* 페이지가 표시됩니다. 이 페이지에서 다음을 수행할 수 있습니다.

- Tivoli Access Manager for WebLogic 사용자를 나열할 수 있습니다.
- 개별 사용자의 세부사항을 표시할 수 있습니다.
- 사용자를 작성할 수 있습니다.

그룹 아이콘을 선택하면 *그룹 관리* 페이지가 표시됩니다. 이 페이지에서 다음을 수행할 수 있습니다.

- 그룹을 나열할 수 있습니다.
- 특정 그룹의 세부사항을 표시할 수 있습니다.
- 그룹을 작성할 수 있습니다.

관련 콘솔 확장 페이지에서 공백으로 구분된 목록을 입력하여 다중 사용자를 그룹에 추가하거나 그룹을 사용자에 추가할 수 있습니다.

사용자 또는 그룹을 나열할 때 *최대 리턴* 필드에 값이 입력되지 않은 경우, *패턴* 필드에 지정된 기준을 충족하는 모든 사용자 또는 그룹이 표시됩니다.

데모 어플리케이션 사용

데모 어플리케이션을 사용하면, 두 가지 유형의 권한 예제를 보고 WebSEAL 싱글 사인 온 기능을 연습할 수 있습니다.

두 가지 유형의 권한은 다음과 같습니다.

- 선언

  배치 디스크립터를 사용하여 사용자 및 그룹 특정 역할을 부여합니다.
- 프로그램

  어플리케이션 소스 코드 내에서 역할 점검이 수행됩니다.

데모 어플리케이션은 웹 구성요소와 EJB 구성요소로 이루어져 있습니다.

웹 구성요소의 두 가지 보안 레벨은 다음과 같이 설명할 수 있습니다.

- 선언:

  `web.xml` 배치 디스크립터는 **ServletRole**이라는 단일 역할을 정의합니다.
  `weblogic.xml` 배치 디스크립터는 **ServletRole**과 **BankMembersServlet** 그룹 간의 프린시펄(사용자) 맵핑을 정의합니다. `web.xml` 배치 디스크립터의 보안 제한 조건은 사용자가 Servlet의 메소드에 액세스하려면 반드시 **ServletRole** 역할이 부여되어야 한다는 것을 나타냅니다.
- 프로그램:

doPost() 메소드는 이때 호출자가 **ServletRole**이 부여되었는지 프로그램으로 확인하는 추가 보안 기능을 가집니다. 이를 사용하면 단일 웹 구성요소 내에 프로그램 및 선언 보안을 둘다 테스트할 수 있습니다. 권한 점검을 수행하려면 HTTPRequest.isUserInRole() 메소드를 사용합니다.

EJB 구성요소의 세 가지 보안 레벨은 다음과 같이 설명할 수 있습니다.

- 선언 보안:

  EJBRole이라는 ejb-jar.xml 배치 디스크립터 내에 단일 역할이 정의됩니다. weblogic-ejb-jar.xml 배치 디스크립터는 **EJBRole** 그룹과 **BankMembersEJB** 그룹 간의 프린시펄 맵핑을 정의합니다. ejb-jar.xml 배치 디스크립터의 메소드 권한은 사용자가 getBalance() 메소드에 액세스하려면 반드시 **EJBRole** 역할이 부여되어야 한다는 것을 나타냅니다.

- 프로그램 보안:

  getBalance() 메소드는 호출자가 **EJBRole**이 부여되었는지 프로그램으로 확인하는 추가 보안 기능을 가집니다. 권한 점검을 수행하려면 EJBContext.isCallerInRole() 메소드를 사용합니다.

- 계정 이름에 따른 프로그램 보안:

  getBalance() 메소드는 요청된 계정의 이름이 호출 프린시펄(사용자)의 이름과 일치하는지 확인합니다. 즉, **Banker1**만 **Banker1**의 계정 밸런스를 볼 수 있어야 합니다.

데모 어플리케이션을 실행하려면 다음 단계를 완료하십시오.

1. 데모 어플리케이션 PDDemoApp.ear을 *WebLogic_domain_directory*\applications로 복사하십시오. 반드시 이 디렉토리를 사용할 필요는 없습니다. EAR 파일을 파일 시스템의 모든 디렉토리에 둘 수 있습니다. 데모 어플리케이션은 *AMWLS_install_dir*/demo에서 찾을 수 있습니다.
2. BEA WebLogic Server 콘솔을 사용하여 다음 사용자를 작성하십시오.

   ```
   Banker1
   Banker2
   Banker3
   Banker4
   URLUser1
   URLUser2
   URLUser3
   ```

3. 두 개의 그룹 *BankMembersEJB* 및 *BankMembersServlet*을 작성하십시오. 새로 작성된 그룹에 사용자 Banker1, Banker2, Banker3 및 Banker4를 추가하십시오.

   BEA WebLogic Server 콘솔 사용에 대한 지시사항은 BEA WebLogic Server 문서를 참조하십시오.

4. BEA WebLogic Server 콘솔을 사용하여 데모 어플리케이션을 배치하십시오.
5. 데모 어플리케이션에 액세스하려면 다음 URL에 액세스하십시오.

http://*WebLogic_Server_host*:*WebLogic_Server_listening_port*/pddemo/PDDemo

위에 정의된 Banker 사용자 중 하나로 인증하십시오.

*WebLogic_Server_host*는 BEA WebLogic Server 시스템의 호스트 이름입니다.

*WebLogic_Server_listening_port*는 BEA WebLogic Server가 인식 중인 포트입니다.

6. **BankMembersServlet** 그룹에 있는 사용자만 Servlet에 액세스할 수 있는지 검증하십시오.
7. **BankMembersEJB** 그룹의 구성원인 인증된 사용자가 자신의 밸런스를 볼 수 있지만 다른 사용자의 밸런스를 볼 수 없는지 검증하십시오.

WebSEAL 싱글 사인 온을 테스트하려면 다음 단계를 완료하십시오.

1. 다음 URL에 액세스하십시오.

   https://*webseald_server_name*/*junction_target*/pddemo/PDDemo

   WebSEAL에서는 인증하라는 프롬프트를 표시합니다.

   변수 *webseald_server_name* 및 *junction_target*에 대한 설명은 34 페이지의 『제 7 부: 구성 테스트』를 참조하십시오.

   주: 기본 WebSEAL 작동으로 인해 HTTP를 통한 기본 또는 양식 기반 인증이 금지되므로 HTTPS를 사용하십시오.
2. 위에 정의된 사용자 중 하나로 인증하십시오.

   이 프로세스는 사용자를 BEA WebLogic Server로 싱글 사인 온하며, 두 번째 인증을 요구하지 않고 Servlet을 호출합니다. WebSEAL을 통해 액세스한 경우, PDDemo 데모 어플리케이션은 BEA WebLogic Server에 직접 액세스할 때 표시되는 것과 동일한 작동을 보여줍니다.
3. 인증된 사용자가 자신의 잔액을 볼 수 있지만 다른 사용자의 잔액은 볼 수 없는지 확인하십시오.

사용 팁

1. 외부 사용자가 싱글 사인 온을 사용할 때 보안 규칙을 잘 지키십시오. WebSEAL 서버만이 인증을 수행해야 합니다. 이를 수행하려면, 내부 사용자, 즉, WebSEAL을 사용하여 BEA WebLogic Server에 액세스하지 않는 사용자 BEA WebLogic Server에 액세스하지 못하도록 하십시오. 이는 네트워크 연결 필터를 사용하여 수행할 수 있습니다. 연결 필터를 사용하면 액세스를 제한하기 위한 역할을 사용하는 대신 네트워크 레벨에서 자원을 보호할 수 있습니다.
2. Tivoli Access Manager와 WebLogic Server 모두 실패한 인증 시도의 트랙을 보존합니다. 각 제품은 사용자 계정이 잠기기 전에 허용 가능한 최대 시도 실패 횟수

를 지정하는 보안 구성 설정을 유지보수합니다. 사용자는 두 설정 중에서 작은 설정에 의해 잠깁니다. 예를 들어, WebLogic 서버가 5번의 로그인 실패를 허용하지만 Tivoli Access Manager가 세 번의 로그인 실패만 허용하도록 구성된 경우, 사용자는 세 번의 로그인 실패 후 잠깁니다.

3회 시도 로그온 policy

LDAP 기반 Tivoli Access Manager 설치에 사용할 수 있는 3회 시도 로그온 policy를 사용하면 최대 로그온 시도 실패 횟수 및 페널티 잠금 시간을 지정하여 컴퓨터 암호 공격을 예방할 수 있습니다. Policy는 로그온 시도 실패가 더 만들어지기까지 일정 시간 대기해야 하는 조건을 작성합니다. 예를 들어, policy는 3회의 실패 시도를 지시할 수 있으며 그 뒤에는 180초의 페널티가 뒤따릅니다. 이 로그온 policy 유형은 컴퓨터가 임의로 생성하는 로그온 시도가 1초에 여러 번 발생되지 못하게 할 수 있습니다.

3회 시도 로그온 policy를 설정하려면 두 개의 **pdadmin** policy 명령 설정이 필요합니다.

- 최대 로그온 시도 실패 횟수
  최대 로그인 실패 수 설정 policy
- 로그온 시도 실패 설정 초과에 대한 페널티
  사용 불가능 시간 간격 설정 policy
  페널티 설정은 계정 잠금 시간 간격 또는 해당 계정의 완전 사용 불가능을 포함할 수 있습니다.

로그온 policy가 특정 잠금 시간 페널티가 부과되는 3회 시도 실패에 대해 설정된 경우(예로서), 네 번째 시도(올바르거나 올바르지 않은)를 하면, 암호 policy 때문에 계정이 임시로 사용 불가능함을 나타내는 오류 메시지가 표시됩니다.

시간 간격은 초로 지정됩니다. 최소 권장 시간 간격은 60초입니다.

사용 불가능 시간 간격 policy가 사용 불가능으로 설정되면, 사용자의 해당 계정이 잠겨지고 이 사용자에 대한 LDAP **유효한 계정** 속성은 아니오로 설정됩니다. 관리자는 Web Portal Manager를 통해 계정을 다시 사용 가능으로 설정합니다.

주: 사용 불가능 시간 간격을 사용 불가능으로 설정하면 추가 관리 오버헤드가 발생합니다. **유효한 계정** 정보를 플러그인에 복제할 때 지연되는 것을 보게 될 수 있습니다. 이러한 상황은 LDAP 환경에 따라 다릅니다. 그 밖에, 특정 LDAP 구현이 **유효한 계정** 갱신 조작의 결과로 성능이 떨어지는 것을 경험하게 될 수 있습니다. 이러한 이유로 시간초과 간격을 사용할 것을 권장합니다.

다음 **pdadmin** 명령은 LDAP 레지스트리에 대해 사용할 때만 적절합니다.

표 3. pdadmin LDAP 로그온 policy 명령

명령	설명
policy set max-login-failures {*number***|unset} [-user** *username***]**	
policy get max-login-failures [-user *username***]**	
	페널티가 부과되기 전까지 허용되는 최대 로그온 시도 실패 횟수를 제어하는 policy를 관리합니다. 이 명령은 policy 설정 사용 불가능 시간 간격 명령에 설정된 페널티에 따라 결정됩니다. 관리자로서 이 policy를 특정 사용자에게 적용하거나 LDAP 레지스트리에 나열된 모든 사용자에게 policy를 전역으로 적용할 수 있습니다. 기본 설정은 10회 시도입니다.
policy set disable-time-interval {*number***|unset|disable} [-user** *username***]**	
policy get disable-time-interval [-user *username***]**	
	최대 로그온 시도 실패 횟수에 도달하면 계정을 사용 불가능하게 하는 시간 기간을 제어하는 페널티 policy를 관리합니다. 관리자로서 이 페널티 policy를 특정 사용자에게 적용하거나 LDAP 레지스트리에 나열된 모든 사용자에게 policy를 글로벌로 적용할 수 있습니다. 기본 설정은 180초입니다.

Tivoli Access Manager 범위 삭제

Tivoli Access Manager 범위를 삭제하려면 다음을 수행하십시오.

1. BEA WebLogic Server가 시작되었는지 확인하십시오.
2. 콘솔을 사용하여 Tivoli Access Manager for WebLogic **create_realm** 조치로 작성되지 않은 기본 범위를 변경하십시오.
3. BEA WebLogic Server를 다시 시작하십시오.
4. 콘솔을 사용하여 Tivoli Access Manager 범위를 삭제하려면 다음을 수행하십시오.
   a. BEA WebLogic Server 탐색줄에서 *Access Manager* 아이콘을 여십시오.
   b. **범위** 아이콘을 누르십시오. *범위 구성* 페이지가 표시됩니다.
   c. **삭제**를 누르십시오. *범위 구성 삭제* 페이지가 표시됩니다.
   d. **확인**을 누르십시오. *범위 작성* 페이지가 빈 필드와 함께 표시됩니다.
5. 명령행을 사용하여 Tivoli Access Manager 범위를 삭제하려면 `AMWLSConfigure -action delete_realm`을 사용하십시오. `AMWLSConfigure -action delete_realm` 명령에 사용할 옵션에 대한 자세한 내용은 63 페이지의 부록 B『명령 빠른 참조』를 참조하십시오.

주: 파일 추출 중 Tivoli Access Manager for WebLogic이 권장 위치에 설치되지 않은 경우, **AMWLSConfigure** 스크립트의 AMSSPI_DIR 변수를 반드시 실제 설치 디렉토리의 위치로 설정하십시오. 마찬가지로, WebLogic이 기본 위치에 설치되지 않았으면, WLS_JAR 변수를 **ALWLSConfigure** 스크립트에 있는 WebLogic.jar의 올바른 위치로 갱신하십시오.

Tivoli Access Manager for WebLogic 구성 해제

Tivoli Access Manager for WebLogic을 구성 해제하려면 다음을 수행하십시오.

1. BEA WebLogic Server가 시작되었는지 확인하십시오.
2. Tivoli Access Manager 범위가 삭제되었는지 확인하십시오. 45 페이지의 『Tivoli Access Manager 범위 삭제』를 참조하십시오.
3. 콘솔을 사용하여 Tivoli Access Manager for WebLogic을 구성 해제하려면 다음을 수행하십시오.
   a. *Access Manager* 폴더를 누르십시오. *구성* 페이지가 표시됩니다.
   b. **삭제**를 누르십시오. *구성 해제* 페이지가 표시됩니다.
   c. Tivoli Access Manager sec_master 암호를 입력하고 **확인**을 누르십시오.
   d. *구성* 페이지가 빈 필드와 함께 표시됩니다.
4. 명령행에서 Tivoli Access Manager for WebLogic을 구성 해제하려면 AMWLSConfigure -action unconfig 명령을 사용하십시오. AMWLSConfigure -action unconfig 명령에 사용할 옵션에 대한 자세한 내용은 63 페이지의 부록 B 『명령 빠른 참조』를 참조하십시오.

문제점 해결 팁

이 절은 다음 주제로 구성되어 있습니다.

- 『양식 기반 로그인을 사용하는 싱글 사인 온 실패』
- 47 페이지의 『WebLogic 서버에 메모리 예외가 발생함』

양식 기반 로그인을 사용하는 싱글 사인 온 실패

사용자가 양식 기반 로그인을 통해 인증되었을 때 권한이 없는 자원에 액세스하려고 시도하는 경우, 다음 오류 메시지가 표시될 수 있습니다.

WebSEAL로부터 메시지를 사인 온할 수 없습니다.

사용자가 실제로 인증될 수 있는 경우에도 웹 컨테이너의 Servlet에 액세스할 권한이 없으므로 이러한 경우가 발생할 수 있습니다.

기본 인증을 사용할 때 이러한 오류가 발생할 경우, 위의 메시지가 아닌 인증 세부사항에 대한 프롬프트가 사용자에게 표시됩니다. 이는 기본 BEA WebLogic Server 작동이며 사용자가 직접 또는 WebSEAL을 통해 페이지에 액세스하는 경우 표시됩니다.

WebLogic 서버에 메모리 예외가 발생함

문제점: `java.lang.OutofMemory` 예외가 발생했습니다.

설명: 다수의 Access Manager for WebLogic Server 세션을 실행 중인 경우, BEA WebLogic Server에 힙 공간이 부족할 수 있습니다.

해결책: startWebLogic 스크립트에서 JVM(Java Virtual Machine)에 대한 최대 힙 *크기* 옵션을 늘리십시오. 예를 들면, 다음과 같습니다.

```
%JAVA_HOME%\bin\java -ms64m -mx128m -xms200m -xx:MaxPermSize=128m
```

어플리케이션 구조, 호스트 시스템에서 실행 중인 메모리 집중 프로세스의 수 및 BEA WebLogic Server의 버전에 따른 권장 힙 *크기*에 대해서는 BEA 제품 문서를 참조하십시오. 어플리케이션 환경의 해당 힙 *크기*를 판별하려면 어플리케이션을 테스트해야 합니다.

제한사항

1. Tivoli Access Manager for WebLogic은 순환 그룹 구성원(그룹 내의 그룹)을 지원하지 않습니다.
2. Tivoli Access Manager for WebLogic은 다중 Tivoli Access Manager 도메인을 지원하지만 각 도메인에 대한 sec_master 사용자는 sec_master여야 합니다. 즉, 각 Tivoli Access Manager 도메인에 대한 이 사용자 이름을 변경하기 위한 옵션이 현재 제공되지 않습니다.
3. BEA WebLogic Server 8.1에서는 그룹 이름에 ″-″ 문자가 지원되지 않으므로 그룹 이름으로 *any-other* 대신 *anyother*를 사용하십시오.
4. Active Directory에 대해 Tivoli Access Manager for WebLogic을 구성할 때, `AdminGroupProp=Administrators` 설정을 다른 설정으로 변경해야 합니다. 이는 Active Directory에 **administrators** 그룹이 이미 존재하므로 구성이 실패하기 때문입니다. Tivoli Access Manager for WebLogic을 구성하고 Tivoli Access Manager for WebLogic 범위를 작성하기 전에 반드시 이를 수행해야 합니다.
5. Tivoli Access Manager for WebLogic 콘솔을 사용하여 역할 및 policy를 작성할 때는 시간 제한사항이 지원되지 않습니다. policy 또는 역할에는 사용자 또는 그룹을 추가할 수 없습니다. 역할과 policy 사이에는 ″OR″만 사용할 수 있으며, ″AND″는 지원되지 않습니다.

6. Tivoli Access Manager는 기본적으로 두 시간 동안 사용자 권한 정보를 캐시합니다. PdPerm.properties의 appsvr-credcache-life 특성을 갱신하여 이 시간 값을 구성할 수 있습니다.
7. WebLogic Server Console Extension에 대한 Tivoli Access Manager Plug-in for Web Servers 또는 WebSEAL에서 싱글 사인 온이 지원되지 않습니다. 그러나 인터넷에서 액세스하는 사용자는 일반적으로 WebLogic 서버 콘솔을 사용할 수 없으므로 이는 큰 문제가 되지 않습니다.

알려진 문제점 및 문제해결 방법

1. Active Directory 사용자 레지스트리를 사용하여 설치하면 인증 어플리케이션을 배치할 때 문제가 발생할 수 있습니다. 이 문제점은 Administrator 그룹 및 시스템 사용자에 대해 하드코드된 역할 맵핑에 의한 것입니다. Active Directory에서 Administrator 그룹 및 시스템 사용자는 사전 정의된 것이므로 제거할 수 없습니다. 이들 오류를 제거하고 인증 어플리케이션에 올바른 보안이 배치되도록 하려면, certificate.war 웹 어플리케이션의 배치 디스크립터를 편집하여 해당 맵핑을 제거하고 실제 Administrator 그룹 및 시스템 사용자에 해당하는 맵핑을 추가하십시오.
2. BEA WebLogic Server 버전 8.1에는 Tivoli Access Manager for WebLogic이 콘솔에서 policy 갱신을 수행할 수 있도록 허용하지 않는 문제점이 있습니다. 이 문제점의 BEA WebLogic Server 변경 요청(CR) 번호는 CR125113입니다. BEA WebLogic Server 8.1 서비스 팩에서 이 문제점이 정정될 때까지 콘솔을 사용한 policy 갱신은 지원되지 않습니다.

제 6 장 제거 지시사항

이 장에서는 IBM Tivoli Access Manager for WebLogic Server를 제거하는 방법에 대해 설명합니다.

다음 절의 지시사항을 완료하십시오.

- 『Solaris에서 제거』
- 50 페이지의 『Windows에서 제거』
- 50 페이지의 『AIX에서 제거』
- 51 페이지의 『HP-UX에서 제거』

Solaris에서 제거

Tivoli Access Manager for WebLogic의 제거를 진행하기 전에 Tivoli Access Manager 범위를 삭제하고 Tivoli Access Manager for WebLogic을 구성 해제했는지 확인하십시오. 이들 태스크의 수행에 대한 자세한 내용은 45 페이지의 『Tivoli Access Manager 범위 삭제』 및 46 페이지의 『Tivoli Access Manager for WebLogic 구성 해제』를 참조하십시오.

Solaris에서 Tivoli Access Manager for WebLogic을 제거하려면 **pkgrm**을 사용하십시오. 다음 지시사항을 완료하십시오.

1. *root*로 로그인하십시오.
2. Tivoli Access Manager for WebLogic을 제거하려면 다음 명령을 입력하십시오.

   ```
   # pkgrm PDWLS
   ```

   선택한 패키지의 제거를 확인하는 프롬프트가 표시됩니다. **y**를 입력하십시오.
3. 제거 프로세스 동안 스크립트가 super 사용자 권한으로 실행될 것을 알리는 경고가 표시됩니다. **y**를 입력하십시오.

파일이 제거될 때 각 파일이 상태 메시지에 나열됩니다. postremove 스크립트가 실행된 후, 소프트웨어 패키지가 제거되었다는 상태 메시지가 표시됩니다. **pkgrm** 유틸리티가 종료됩니다.

Tivoli Access Manager for WebLogic 패키지가 제거되었습니다.

IBM Tivoli Access Manager 기본 사전 설치 소프트웨어(Tivoli Access Manager 기본 런타임 환경, Tivoli Access Manager 기본 JRE(Java Runtime Environment) 및 선택적 Tivoli Access Manager 어플리케이션 개발 킷)를 제거하려면 *IBM Tivoli Access Manager 기본 설치 안내서*를 참조하십시오.

© Copyright IBM Corp. 2003

Windows에서 제거

Tivoli Access Manager for WebLogic의 제거를 진행하기 전에 Tivoli Access Manager 범위를 삭제하고 Tivoli Access Manager for WebLogic을 구성 해제했는지 확인하십시오. 이들 태스크의 수행에 대한 자세한 내용은 45 페이지의 『Tivoli Access Manager 범위 삭제』 및 46 페이지의 『Tivoli Access Manager for WebLogic 구성 해제』를 참조하십시오.

Windows 프로그램 추가/제거 아이콘 인터페이스를 사용하여 Tivoli Access Manager for WebLogic 파일을 제거하십시오. 다음 지시사항을 완료하십시오.

1. 관리자 권한이 있는 Windows 사용자로 로그인하십시오.
2. **프로그램 추가/제거** 아이콘을 두 번 누르십시오.
3. **Access Manager for WebLogic Application Server**를 선택하십시오.
4. **변경/제거**를 누르십시오.

   Tivoli Access Manager for WebLogic 파일이 제거됩니다.

   유지보수관리 완료 대화 상자가 표시됩니다.
5. **확인**을 누르십시오.

Tivoli Access Manager for WebLogic이 제거되었습니다.

IBM Tivoli Access Manager 기본 사전 설치 소프트웨어(Tivoli Access Manager 기본 런타임 환경, Tivoli Access Manager 기본 JRE(Java Runtime Environment) 및 선택적 Tivoli Access Manager 어플리케이션 개발 킷)를 제거하려면 *IBM Tivoli Access Manager 기본 설치 안내서*를 참조하십시오.

AIX에서 제거

Tivoli Access Manager for WebLogic의 제거를 진행하기 전에 Tivoli Access Manager 범위를 삭제하고 Tivoli Access Manager for WebLogic을 구성 해제했는지 확인하십시오. 이들 태스크의 수행에 대한 자세한 내용은 45 페이지의 『Tivoli Access Manager 범위 삭제』 및 46 페이지의 『Tivoli Access Manager for WebLogic 구성 해제』를 참조하십시오.

AIX 패키지에 대한 Tivoli Access Manager for WebLogic을 제거하려면 **installp** 유틸리티를 사용하십시오.

IBM Tivoli Access Manager 기본 사전 설치 소프트웨어(Tivoli Access Manager 기본 런타임 환경, Tivoli Access Manager 기본 JRE(Java Runtime Environment) 및 선택적 Tivoli Access Manager 어플리케이션 개발 킷)를 제거하려면 *IBM Tivoli Access Manager 기본 설치 안내서*를 참조하십시오.

HP-UX에서 제거

Tivoli Access Manager for WebLogic의 제거를 진행하기 전에 Tivoli Access Manager 범위를 삭제하고 Tivoli Access Manager for WebLogic을 구성 해제했는지 확인하십시오. 이들 태스크의 수행에 대한 자세한 내용은 45 페이지의 『Tivoli Access Manager 범위 삭제』 및 46 페이지의 『Tivoli Access Manager for WebLogic 구성 해제』를 참조하십시오.

swremove를 사용하여 Tivoli Access Manager for WebLogic 파일을 제거하십시오. 다음 지시사항을 완료하십시오.

1. *root*로 로그인하십시오.
2. Tivoli Access Manager for WebLogic을 제거하려면 다음 명령을 입력하십시오.

   ```
   # swremove PDWLS
   ```

   일련의 상태 메시지가 표시됩니다. 분석 단계가 완료되었음을 알리는 상태 메시지가 표시됩니다. **swremove** 유틸리티는 하드 디스크에서 Tivoli Access Manager for WebLogic 파일을 제거합니다.

   제거가 완료되면, **swremove** 유틸리티가 종료됩니다.

이제 HP-UX에서 Tivoli Access Manager for WebLogic이 제거되었습니다.

IBM Tivoli Access Manager 기본 사전 설치 소프트웨어(Tivoli Access Manager 기본 런타임 환경, Tivoli Access Manager 기본 JRE(Java Runtime Environment) 및 선택적 Tivoli Access Manager 어플리케이션 개발 킷)를 제거하려면 *IBM Tivoli Access Manager 기본 설치 안내서*를 참조하십시오.

부록 A. 특성 파일 참조

Tivoli Access Manager for WebLogic을 구성하고 범위를 작성할 때 입력되는 데이터는 특성 파일에 저장됩니다. 이들 특성 파일은 Tivoli Access Manager for WebLogic의 작동을 변경하는 데 사용할 수 있습니다.

특성 파일은 *java_home*/amwls/*wls_domain_name*/*wls_realm_name*/에 존재합니다. 여기서 *wls_domain_name*은 구성된 BEA WebLogic Server 도메인의 이름이고 *wls_realm_name*은 이 도메인 내에 구성된 BEA WebLogic Server 범위의 이름입니다.

다음과 같이 세 개의 특성 파일이 있습니다.

- amsspi.properties
  BEA WebLogic Server에 특정한 SSPI 기능에 대한 구성 특성이 들어 있습니다.
- rbpf.properties
  Tivoli Access Manager for WebLogic에 대한 구성 특성이 들어 있습니다. 예를 들어, 캐시 설정, 역할 특성 및 Tivoli Access Manager 보호 오브젝트 공간 컨테이너 이름입니다.
- amwlsjlog.properties
  이 파일에 있는 매개변수는 수행된 추적/메시지의 양을 포함하여 Tivoli Access Manager for WebLogic에 대한 로깅 및 추적을 제어합니다. 추적을 활성화하면 Tivoli Access Manager for WebLogic의 성능에 영향을 줄 수 있다는 점을 주지하십시오. 문제점의 원인을 판별하려고 시도할 때만 추적을 활성화할 것을 권장합니다.

다음 절에서는 각 특성 파일에 있는 매개변수에 대해 설명합니다.

*** 표시는 Tivoli Access Manager for WebLogic을 구성할 때 입력되지 않는 특성을 나타냅니다. 이들 특성은 구성 시간에 기본값으로 설정됩니다. 이들 값을 기본값 이외의 다른 값으로 설정하려면 범위를 작성 및 구성하기 전에 해당 .in 파일에 있는 특성 값을 변경해야 합니다. **config** 및 **create_realm** 조치는 .in 파일의 값을 사용하여 ACL 및 Tivoli Access Manager 보호 오브젝트를 작성하므로 구성하거나 범위를 작성한 후에는 변경할 수 없습니다. 다음 절에서 ***로 표시되지 않은 특성은 구성 이후에 쉽게 변경할 수 있습니다.

.in 파일은 *pdwls_install_dir*/etc에서 찾을 수 있습니다.

amsspi.properties

이 절에서는 amsspi.properties 파일에 있는 특성을 나열하고 설명합니다.

© Copyright IBM Corp. 2003

com.tivoli.amwls.sspi.config.DeployerGroupProp***

기본값은 *Deployers*입니다. 기본적으로, BEA WebLogic Server에는 네 개의 관리 그룹이 있는데, 이 특성은 사용자가 *Deployers* 관리 그룹의 이름을 *Deployers* 이외의 다른 이름으로 변경할 수 있도록 합니다.

com.tivoli.amwls.sspi.config.MonitorGroupProp***

기본값은 *Monitors*입니다. 기본적으로, BEA WebLogic Server에는 네 개의 관리 그룹이 있는데, 이 특성은 사용자가 *Monitors* 관리 그룹의 이름을 *Monitors* 이외의 다른 이름으로 변경할 수 있도록 합니다.

com.tivoli.amwls.sspi.config.OperatorGroupProp***

기본값은 *Operators*입니다. 기본적으로, BEA WebLogic Server에는 네 개의 그룹이 있는데, 이 특성은 사용자가 Operators 관리 그룹의 이름을 Operators 이외의 다른 이름으로 변경할 수 있도록 합니다.

com.tivoli.amwls.sspi.config.AdminGroupProp***

기본값은 *Administrators*입니다. 기본적으로, BEA WebLogic Server에는 네 개의 관리 그룹이 있는데, 이 특성은 사용자가 *Administrator* 관리 그룹의 이름을 *Administrators* 이외의 다른 이름으로 변경할 수 있도록 합니다. Windows가 이미 *Administrators*라는 관리 그룹을 이미 가지고 있기 때문에 이 특성을 갱신해야 하므로 Active Directory를 사용하는 시스템에 대해 중요한 특성입니다.

com.tivoli.amwls.sspi.Authentication.GroupRegistryDelete

기본값은 *true*입니다. 이 특성은 Tivoli Access Manager 그룹이 삭제될 때 기본 디렉토리에서 그룹이 삭제되는지 여부를 결정합니다. 이는 **pdadmin**을 사용하여 그룹을 삭제할 때 **-registry** 플래그를 켜고 끄는 것과 동일합니다.

com.tivoli.amwls.sspi.Authentication.UserRegistryDelete

기본값은 *true*입니다. 이는 Tivoli Access Manager 사용자가 삭제될 때 기본 디렉토리에서 사용자가 삭제되는지 여부를 결정합니다. 이는 **pdadmin**을 사용하여 사용자를 삭제할 때 **-registry** 플래그를 켜고 끄는 것과 동일합니다.

com.tivoli.amwls.sspi.Authentication.ssoEnabled

기본값은 *false*입니다. BEA WebLogic Server에 대한 Tivoli Access Manager Plug-in for Web Servers 또는 WebSEAL에서 싱글 사인 온을 사용 가능/사용 불가능으로 설정합니다.

com.tivoli.amwls.sspi.Authentication.ssoTrustId

싱글 사인 온을 수행하기 위해 WebSEAL 또는 Tivoli Access Manager Plug-in for Web Servers와 신뢰 연관을 확립하는 데 사용되는 사용자

com.tivoli.amwls.sspi.Authentication.ssoPasswdExpiry

기본값은 120(분)입니다. 이 특성은 SSO 신뢰 ID의 인증이 캐시되는 시간(분)을 지정합니다. 이 시간이 완료되면, SSO 사용자는 다음 번 SSO 시도 시 Tivoli Access Manager에 대해 인증됩니다.

com.tivoli.amwls.sspi.RoleMapper.EnableWebProgRolecheck

기본값은 *true*입니다. 이 특성은 웹 프로그램식 역할 점검을 사용 가능 또는 사용 불가능하게 합니다. 이 특성은 관리자가 웹 어플리케이션에 대한 프로그램식 보안을 끌 수 있도록 합니다.

com.tivoli.amwls.sspi.RoleMapper.EnableEjbProgRolecheck

기본값은 *true*입니다. 이 특성은 EJB 프로그램식 역할 점검을 사용 가능 또는 사용 불가능하게 합니다. 이 특성은 관리자가 EJB에 대한 프로그램식 보안을 끌 수 있도록 합니다.

com.tivoli.amwls.sspi.Authentication.GroupDNPrefix

LDAP의 경우, 기본값은 cn=입니다. 이 특성은 콘솔 확장으로부터 그룹을 작성할 때 관리자가 접두어를 변경할 수 있도록 합니다.

com.tivoli.amwls.sspi.Authentication.UserDNPrefix

LDAP의 경우, 기본값은 cn=입니다. 이 특성은 콘솔 확장으로부터 사용자를 작성할 때 관리자가 접두어를 변경할 수 있도록 합니다.

rbpf.properties

이 절에서는 `rbpf.properties` 파일에 있는 특성을 나열하고 설명합니다.

com.tivoli.pd.as.rbpf.ProductName

기본값은 *PDWLS*입니다. Tivoli Access Manager 오브젝트 및 ACL을 작성할 때 주석 및 설명에서 이 특성을 사용합니다.

com.tivoli.pd.as.rbpf.RoleContainerName***

기본값은 *Roles*입니다. 구성 후, 이 특성은 `Roles/$WLS_Domain_Name/$WLS_Realm_Name`으로 변경됩니다. 여기서 *WLS_Domain_Name*은 구성된 BEA WebLogic Server 도메인의 이름이고, *WLS_Realm_Name*은 구성된 BEA WebLogic Server 범위의 이름입니다.

com.tivoli.pd.as.rbpf.ResourceContainerName***

기본값은 *Resources*입니다. 구성 후, 이 특성은 `Resources/$WLS_Domain_Name/$WLS_Realm_Name`으로 변경됩니다. 여기서 *WLS_Domain_Name*은 구성된 BEA WebLogic Server 도메인의 이름이고, *WLS_Realm_Name*은 구성된 BEA WebLogic Server 범위의 이름입니다.

com.tivoli.pd.as.rbpf.PosRoot***

기본값은 *WebAppServer*입니다. 이 특성은 Tivoli Access Manager for WebLogic에 있는 모든 역할 및 자원에 대한 오브젝트 공간의 절대 루트입니다.

com.tivoli.pd.as.rbpf.ProductId***

기본값은 *WLS*입니다. 이 특성은 **PosRoot** 값과 결합하여 모든 역할 및 자원에 대한 오브젝트 공간의 루트를 형성합니다.

com.tivoli.pd.as.rbpf.AMActionGroup***

기본값은 *WebAppServer*입니다. 이 특성은 Tivoli Access Manager for WebLogic 액세스 결정이 점검할 조치를 저장하는 데 사용되는 조치 그룹의 기본 이름입니다.

com.tivoli.pd.as.rbpf.AMAction***

기본값은 호출(invoke)에 대한 *i*입니다. 이 조치는 Tivoli Access Manager for WebLogic이 액세스 결정을 수행할 때 점검되며, *AMActionGroup*에 추가됩니다.

com.tivoli.pd.as.cache.EnableDynamicRoleCaching

기본값은 *true*입니다. 이 특성은 동적 역할 캐싱을 사용 가능 또는 사용 불가능하게 합니다. 모든 보통 역할, 즉, 관리 역할 이외의 역할을 캐시하려면 동적 역할 캐시를 사용합니다. 긍정 및 부정 역할 구성원을 캐시합니다.

com.tivoli.pd.as.cache.DynamicRoleCache

기본값은 *com.tivoli.pd.as.cache.DynamicRoleCacheImpl*입니다. 이 특성은 동적 역할 캐싱을 수행하는 데 사용되는 클래스입니다. 필요한 경우, 사용자의 동적 역할 캐시를 구현할 수 있습니다. 이는 *com.tivoli.pd.as.cache.IDynamicRoleCache* 인터페이스를 구현하여 수행할 수 있습니다.

com.tivoli.pd.as.cache.DynamicRoleCache.NumBuckets

기본값은 *20*입니다. 이 특성은 동적 역할 캐시 항목을 저장하는 데 사용되는 기본 해시 테이블에서 사용해야 하는 버킷의 수를 지정합니다.

com.tivoli.pd.as.cache.DynamicRoleCache.MaxUsers

기본값은 *100000*입니다. 이 특성은 캐시에 있는 모든 버킷에 대한 총 항목 수입니다. 이 숫자를 *NumBuckets*로 나누면 각 개별 버킷의 *최대 크기*가 결정됩니다.

com.tivoli.pd.as.cache.DynamicRoleCache.RoleLifetime

기본값은 *20*입니다. 이 특성은 긍정 및 부정 동적 역할 캐시 결정이 캐시에 남아 있는 시간(초)을 지정합니다.

com.tivoli.pd.as.cache.DynamicRoleCache.PrincipalLifeTime

기본값은 *10*입니다. 이 특성은 프린시펄(사용자) 권한 정보가 Tivoli Access Manager for WebLogic 캐시에 저장되는 시간(분)을 지정합니다.

PdPerm.properties 값 *appsvr-credcache-life*는 권한 정보가 PDJRTE에 캐시되는 시간을 결정한다는 점을 주지하십시오. Tivoli Access Manager for WebLogic은 PDJRTE에서 모든 권한 정보를 확보합니다. 따라서 이 값이 *appsvr-credcache-life*보다 적을 경우, 이는 Tivoli Access Manager for WebLogic이 PDJRTE에서 캐시된 권한 정보를 검색할 때 겹쳐써집니다.

com.tivoli.pd.as.cache.EnableStaticRoleCaching

기본값은 *true*입니다. 이 특성은 정적 역할 캐싱을 사용 가능 또는 사용 불가능하게 합니다. 정적 약할 캐시는 관리 역할에 대한 긍정 및 부정 역할 구성원을 캐시하는 데 사용됩니다. 이 캐시는 항목이 만료되지 않는 것을 제외하고는 동적 역할 캐시와 동일합니다. 이는 이러한 역할에 대한 구성원이 변경되지 않으므로 관리 역할의 성능을 개선합니다.

com.tivoli.pd.as.cache.StaticRoleCache

기본값은 *com.tivoli.pd.as.cache.StaticRoleCacheImpl*입니다. 이 특성은 정적 역할 캐싱을 수행하는 데 사용되는 클래스입니다. 필요한 경우, 사용자의 정적 역할 캐시를 구현할 수 있습니다. 이는 *com.tivoli.pd.as.cache.IStaticRoleCache* 인터페이스를 구현하여 수행할 수 있습니다.

com.tivoli.pd.as.cache.StaticRoleCache.Roles

기본값은 *Admin, Operator, Monitor, Deployer*입니다. 이 특성은 쉼표로 구분된 관리 역할 목록을 보유합니다. 이 목록에 있는 역할 구성원은 동적 역할 캐시보다는 정적 역할 캐시에 추가됩니다. 기타 모든 역할 구성원은 동적 역할 캐시에 캐시됩니다.

com.tivoli.pd.as.cache.EnableObjectCaching

기본값은 *true*입니다. 이 특성은 오브젝트 캐싱을 사용 가능 또는 사용 불가능하게 합니다. 이 오브젝트 캐시는 확장 속성을 포함한 모든 Tivoli Access Manager 오브젝트를 캐시하는 데 사용됩니다. 이를 사용하여 어떤 BEA WebLogic Server 자원에 대해 어떤 역할이 액세스 부여되는지 캐싱할 수 있으며, 따라서 각 자원 요청에 대해 Tivoli Access Manager Authorization Server를 조회해야 하는 필요성을 생략할 수 있습니다.

com.tivoli.pd.as.cache.ObjectCache

기본값은 *com.tivoli.pd.as.cache.ObjectCacheImpl*입니다. 이 특성은 오브젝트 캐싱을 수행하는 데 사용되는 클래스입니다. 필요한 경우, 사용자의 오브젝트 캐시를 구현할 수 있습니다. 이는 *com.tivoli.pd.as.cache.IObjectCache* 인터페이스를 구현하여 수행할 수 있습니다.

com.tivoli.pd.as.cache.ObjectCache.NumBuckets

기본값은 *20*입니다. 이 특성은 기본 해시 테이블에 오브젝트 캐시 항목을 저장하는 데 사용되는 버킷의 수를 지정합니다.

com.tivoli.pd.as.cache.ObjectCache.MaxResources

기본값은 *10000*입니다. 이 특성은 캐시에 있는 모든 버킷에 대한 총 항목 수를 지정합니다. 이 숫자를 **NumBuckets**로 나누면 각 버킷의 최대 크기가 결정됩니다.

com.tivoli.pd.as.cache.ObjectCache.ResourceLifeTime

기본값은 *20*입니다. 이 특성은 오브젝트 캐시에서 오브젝트가 보존되는 시간(분)을 지정합니다.

com.tivoli.pd.as.rbpf.UncheckedRoles

기본값은 *Unchecked, AmasUnckeched, Anonymous*입니다. 이 특성은 쉼표로 구분된 J2EE 선택 취소 역할 목록을 지정합니다. 나열된 역할 중에서 BEA WebLogic Server 자원에 대한 액세스가 부여되지 않은 역할이 있는 경우, 모든 사용자는 어떤 보통 역할이 첨부되었는지에 관계없이 이에 대한 액세스를 부여받습니다. 사용자와 그룹은 이들 역할에 추가될 수 없습니다. 이들 역할은 모든 사용자(인증되지 않은 사용자 포함)에게 특정 자원에 대한 액세스를 부여하는 효율적인 방법을 표시합니다. Tivoli Access Manager for WebLogic 구성이 이 체크되지 않은 역할을 여러 기본 BEA WebLogic Server 자원에 추가할 때 *Anonymous* 역할은 항상 이 목록에 남아 있어야 합니다. 이 특성은 구성 전에 설정할 필요는 없지만 일단 설정된 후에는 변경하지 않아야 합니다.

com.tivoli.pd.as.rbpf.ExcludedRoles

기본값은 *Excluded, AmasExcluded*입니다. 이 특성은 쉼표로 구분된 J2EE 제외 역할 목록을 지정합니다. 따라서, 이들 역할 중 자원에 첨부된 역할이 있는 경우, 사용자는 어떤 보통 역할이 첨부되었는지에 관계없이 이에 대한 액세스가 부여되지 않습니다. 이들 J2EE 제외 역할은 모든 사용자에 대해 특정 자원에 대한 액세스를 거부하는 효율적인 방법을 표시합니다. 이 특성은 구성 전에 설정할 필요는 없지만 일단 설정된 후에는 변경하지 않아야 합니다.

com.tivoli.pd.as.rbpf.GrantUnprotectedAccess

기본값은 *true*입니다. 이 특성은 보호되지 않는 요청된 자원, 즉, 어떠한 역할도 부여되지 않은 오브젝트에 대해 액세스를 부여 또는 거부할 것인지를 지정합니다.

com.tivoli.pd.as.rbpf.CopyParentRole***

기본값은 *false*입니다. 관리자는 이 특성을 사용하여 보다 특정 레벨의 역할(예: 어플리케이션 레벨의 역할)을 작성할 때 상위 레벨에 정의된 역할 구성원(예: 글로벌 역할)을 복사해야 하는지 여부를 지정할 수 있습니다. Tivoli Access Manager에서 이 특성은 글로벌 레벨에 첨부된 ACL의 모든 구성원을 어플리케이션 레벨의 오브젝트에 첨부된 ACL로 복사하는 작업을 포함합니다. 이 특성은 관리자에게 새 역할을 작성할 때 역할 구성원에 상속의 개념을 적용할 수 있는 기능을 제공합니다. 일반적으로 이 특성은
PropogateChileRole과 동일한 값으로 설정되어야 합니다.

com.tivoli.pd.as.rbpf.PropagateChildRole***

기본값은 *false*입니다. 관리자는 이 특성을 사용하여 상위 레벨에 정의된 역할 구성원(예: 글로벌 역할)에 작성된 변경사항이 하위 역할(예: 어플리케이션 레벨의 역할)에도 작성되는지 여부를 지정할 수 있습니다. 즉, userA를 글로벌 역할 RoleA에 추가할 때 userA를 또한 어플리케이션 레벨의 RoleA에 추가합니다. 이렇게 하면 역할 구성원을 갱신할 때 **CopyParentRole**을 향상시키고 더 나아가 역할 구성원 상속을 적용합니다. 일반적으로 이 특성은 **CopyParentRole**과 동일한 값으로 설정되어야 합니다.

com.tivoli.pd.as.rbpf.UseEntitlements

기본값은 *false*입니다. 이 특성은 어떤 역할에 어떤 자원에 대한 액세스가 부여되었는지에 관한 정보를 수집하는 데 Tivoli Access Manager Authorization Server의 인타이틀먼트 서비스를 사용해야 하는지 여부를 표시합니다. 기본값은 *false*이므로, 최소 Tivoli Access Manager 서비스 수를 설정하여 Tivoli Access Manager for WebLogic을 실행시킬 수 있습니다. 그러나, 이 특성은 Tivoli Access Manager Policy Server에 대해 단일 실패 지점을 가지므로 테스트 환경에서는 *false*로만 설정되어야 합니다. 인타이틀먼트 서비스는 또한 내부 오브젝트 캐싱에 기초하여 훨씬 더 높은 레벨에서 수행합니다. 따라서, 프로덕션 환경에서 이 값은 항상 *true*로 설정되어야 합니다.

com.tivoli.pd.as.rbpf.EntitlementsUser

기본갓은 Tivoli Access Manager for WebLogic remote-acl-user입니다. 이 특성은 인타이틀먼트 서비스를 사용하여 오브젝트 검색을 수행하는 데 사용되는 사용자를 보유합니다. 인타이틀먼트 서비스는 Tivoli Access Manager 보호 오브젝트 공간의 사용자 요청 오브젝트가 서버 관리 일반 ‘s’ 권한을 부여받았는지 확인합니다. **config**를 수행하는 동안 romote-acl-user는 iv-admin 그룹에 추가되고 이 권한이 부여됩니다. 이 사용자를 변경하여 사용자 요청 오브젝트를 갱신할 수 있지만, 이 새 사용자가 Tivoli Access Manager 보호 오브젝트 공간의 *Resources* 컨테이너에 대해 ‘s’ 권한을 부여받았는지 확인해야 합니다.

com.tivoli.pd.as.rbpf.IgnorePasswordPolicyOnUserCreate

기본값은 *false*입니다. 관리자는 이 특성을 사용하여 BEA WebLogic Server 콘솔을 통해 새 Tivoli Access Manager 사용자를 작성할 때 암호 policy를 무시할 수 있습니다.

com.tivoli.pd.as.rbpf.DeleteBaseRoleRecursive

기본값은 *true*입니다. 이 특성은 상위 역할을 삭제할 때 모든 하위 역할을 삭제할 것인지 여부를 표시합니다.

amwlsjlog.properties

amwlsjlog.properties 파일은 표준 JLog 특성 파일입니다. 이 파일은 Tivoli Access Manager for WebLogic과 PDJRTE에서 메시지 전달 및 추적을 제어하는 데 사용됩니다.

amwlsjlog.properties 파일에 포함된 특성이 대부분 이 책의 목적에 적합하지 않으므로 이 절에서는 모든 특성을 나열하지 않습니다. 이 파일에서 메시지 전달 및 추적을 사용 또는 사용 불가능하게 할 수 있습니다.

amwlsjlog.properties 파일의 항목은 계층 구조적입니다. 여러 구성요소에 대한 로깅을 한번에 켜거나 단일 구성요소에 대해 로깅을 켤 수 있습니다.

로깅을 켜려면, 단순히 로깅을 사용 가능하게 하려는 구성요소에 **isLogging** 특성을 추가하십시오. 아래에 나열된 항목은 Tivoli Access Manager for WebLogic이 지원하는 추적 및 메시지 전달 구성요소입니다. 이들 나열된 특성 중 하나 또는 모두에 대해 추적/메시지 전달을 사용 가능하게 할 수 있습니다. 다음은 각 구성요소가 수행하는 작업을 간략하게 설명합니다.

구성요소	설명
추적	
AmasRBPFTraceLogger	Tivoli Access Manager for WebLogic의 내부 조작에 대한 추적
AmasCacheTraceLogger	모든 Tivoli Access Manager for WebLogic 캐시에 대한 조작
AMSSPICfgTraceLogger	Tivoli Access Manager for WebLogic의 **config** 조작에 대한 추적(예: 역할 작성)
AMSSPIAuthzTraceLogger	Tivoli Access Manager for WebLogic의 권한 제공자에 대한 추적
AMSSPIAuthnTraceLogger	Tivoli Access Manager for WebLogic의 인증 제공자에 대한 추적
AMSSPIRoleMapperTraceLogger	Tivoli Access Manager for WebLogic의 역할 맵핑 제공자에 대한 추적
AMSSPIResourceManagerTrace Logger	Tivoli Access Manager for WebLogic 내의 자원 관리자에 대한 추적
메시지 전달	
AmasCacheMessageLogger	Tivoli Access Manager for WebLogic의 내부 조작에 대한 메시지 전달
AmasRBPFMessageLogger	모든 Tivoli Access Manager for WebLogic 캐시에 대한 메시지 전달
AMSSPICfgMessageLogger	Tivoli Access Manager for WebLogic의 **config** 조작에 대한 메시지 전달(예: 역할 작성)
AMSSPIAuthzMessageLogger	Tivoli Access Manager for WebLogic의 권한 제공자에 대한 메시지 전달

구성요소	설명
AMSSPIAuthnMessageLogger	Tivoli Access Manager for WebLogic의 인증 제공자에 대한 메시지 전달
AMSSPIRoleMapperMessage Logger	Tivoli Access Manager for WebLogic의 역할 맵핑 제공자에 대한 메시지 전달
AMSSPIResourceManager MessageLogger	Tivoli Access Manager for WebLogic 내의 자원 관리자에 대한 메시지 전달

위의 각 구성요소는 **baseGroup traceLogger** 및 **baseGroup messageLogger**를 확장합니다. 따라서, 특성 파일에서 이들의 특성은 다음 예제와 유사하게 나타납니다.

```
baseGroup.AMSSPIAuthnMessageLogger.isLogging=true
```

위의 예제는 Tivoli Access Manager for WebLogic의 인증 제공자 섹션에 대한 메시지 전달을 사용 가능하게 합니다. 권한 제공자를 제외한 모든 구성요소에 대한 추적을 사용 가능하게 하려면 다음 라인을 추가하십시오.

```
baseGroup.TraceLogger.isLogging=true
baseGroup.AMSSPIAuthzMessageLogger.isLogging=false
```

즉, 모든 다른 추적 구성요소는 단순히 기본 로그 프로그램에서 *true* 값을 상속합니다. 이에 반해, 권한 로그 프로그램은 *true* 값을 *false*로 겹쳐씁니다.

부록 B. 명령 빠른 참조

© Copyright IBM Corp. 2003

AMWLSConfigure -action config

Tivoli Access Manager for WebLogic Server를 구성합니다.

구문

AMWLSConfigure -action config -domain_admin *domain_admin* **-domain_admin_pwd** *domain_admin_password* **-remote_acl_user** *remote_acl_user* **-sec_master_pwd** *sec_master_pwd* **-pdmgrd_host** *pdmgrd_host* **-pdacld_host** *pdacld_host* **[-deploy_extension {true|false}] [-wls_server_url** *wls_server_url***] [-am_domain** *am_domain***] [-pdmgrd_port** *pdmgrd_port***] [-pdacld_port** *pdacld_port***] [-amwls_home** *amwls_home***] [-verbose {true|false}]**

매개변수

-am_domain *am_domain*

Tivoli Access Manager 도메인의 이름을 지정합니다. 기본 도메인은 **Default**입니다.

-amwls_home *amwls_home*

Tivoli Access Manager for WebLogic Server 설치 디렉토리에 대한 경로를 지정합니다.

-deploy_extension {true|false}

true로 설정할 경우 Tivoli Access Manager Web Logic Server 버전 5.1 콘솔 확장을 배치합니다. 기본값은 **true**입니다.

-domain_admin *domain_admin*

WebLogic 도메인 관리자를 지정합니다.

-domain_admin_pwd *domain_admin_password*

WebLogic 도메인 관리자 암호를 지정합니다.

-pdacld_host *pdacld_host*

Tivoli Access Manager Authorization Server 호스트 이름을 지정합니다.

-pdacld_port *pdacld_port*

Tivoli Access Manager Authorization Server 포트 번호를 지정합니다. 기본 포트 번호는 **7136**입니다.

-pdmgrd_host *pdmgrd_host*

Tivoli Access Manager Policy Server 호스트 이름을 지정합니다.

-pdmgrd_port *pdmgrd_port*

Tivoli Access Manager Policy Server 포트 번호를 지정합니다. 기본 포트 번호는 **7135**입니다.

-remote_acl_user *remote_acl_user*

Authorization Server용으로 작성되는 Tivoli Access Manager 프린시펄(사용자)을 지정합니다.

-sec_master_pwd *sec_master_pwd*

Tivoli Access Manager 관리 사용자 암호(보통 `sec_master`)를 지정합니다.

-verbose {true|false}

true로 설정할 경우 자세한 출력을 사용 가능하게 합니다. 기본값은 **false**입니다.

-wls_server_url *wls_server_url*

로컬 WebLogic 서버에 대한 URL을 지정합니다. 기본값은 `t3://localhost:7001`입니다.

가용성

이 명령은 다음과 같은 기본 설치 디렉토리에 위치합니다.

- UNIX:

  `/opt/pdwls/sbin/`

- Windows 시스템의 경우:

  `C:\Program Files\Tivoli\pdwls\sbin\`

기본값 이외의 다른 설치 디렉토리를 선택할 때, 이 유틸리티는 설치 디렉토리 아래의 `sbin` 디렉토리(예: *`install_dir`*`\sbin\`)에 위치합니다.

리턴 코드

다음과 같은 종료 상태 코드가 리턴될 수 있습니다.

0 명령이 완료되었습니다.

1 명령에 실패했습니다.

명령에 실패하면 오류 메시지가 표시됩니다. 문제점의 자세한 설명에 대해서는 *IBM Tivoli Access Manager Error Message Reference*를 참조하십시오.

AMWLSConfigure -action unconfig

Tivoli Access Manager for WebLogic Server를 구성 해제합니다.

구문

AMWLSConfigure -action unconfig -domain_admin_pwd *domain_admin_pwd* **-sec_master_pwd** *sec_master_pwd* **[-verbose {true|false}]**

매개변수

-domain_admin_pwd *domain_admin_pwd*

Tivoli Access Manager for WebLogic Server 도메인 관리자 암호를 지정합니다.

-sec_master_pwd *sec_master_pwd*

Tivoli Access Manager 관리 사용자 암호(보통 `sec_master`)를 지정합니다.

-verbose {true|false}

true로 설정할 경우 자세한 출력을 사용 가능하게 합니다. 기본값은 **false**입니다.

가용성

이 명령은 다음과 같은 기본 설치 디렉토리에 위치합니다.

- UNIX:

  `/opt/pdwls/sbin/`

- Windows 시스템의 경우:

  `C:\Program Files\Tivoli\pdwls\sbin\`

기본값 이외의 다른 설치 디렉토리를 선택할 때, 이 유틸리티는 설치 디렉토리 아래의 `sbin` 디렉토리(예: *`install_dir`*`\sbin\`)에 위치합니다.

리턴 코드

다음과 같은 종료 상태 코드가 리턴될 수 있습니다.

0 명령이 완료되었습니다.

1 명령에 실패했습니다.

명령에 실패하면 오류 메시지가 표시됩니다. 문제점의 자세한 설명에 대해서는 *IBM Tivoli Access Manager Error Message Reference*를 참조하십시오.

AMWLSConfigure -action create_realm

WebLogic 서버 내에 보안 범위를 작성합니다.

구문

AMWLSConfigure -action create_realm -realm_name *realm_name* **-domain_admin_pwd** *domain_admin_pwd* **-user_dn_suffix** *user_dn_suffix* **-group_dn_suffix** *group_dn_suffix* **-admin_group** *admin_group* **[-user_dn_prefix** *user_dn_prefix***] [-group_dn_prefix** *group_dn_prefix***] [-sso_enabled {true|false}] [-sso_user** *sso_user***] [-sso_pwd** *sso_pwd***] [-verbose {true|false}]**

매개변수

-admin_group *admin_group*
내부 구성 용도에 사용할 Tivoli Access Manager 그룹을 지정합니다.

-domain_admin_pwd *domain_admin_pwd*
WebLogic 도메인 관리자 암호를 지정합니다.

-group_dn_prefix *group_dn_prefix*
그룹을 작성할 때 사용할 구별 이름(DN) 접두어를 지정합니다.

-group_dn_suffix *group_dn_suffix*
그룹을 작성할 때 사용할 구별 이름(DN) 접미어를 지정합니다.

-realm_name *realm_name*
작성 중인 WLS 범위의 이름을 지정합니다.

-sso_enabled {true|false}
true로 설정할 경우 싱글 사인 온 보조 관리자를 사용 가능하게 합니다. 기본값은 **false**입니다.

-sso_pwd *sso_pwd*
싱글 사인 온 사용자(*sso_user*)의 암호를 지정합니다.

-sso_user *sso_user*
Tivoli Access Manager와 싱글 사인 온 신뢰 연관을 작성하기 위한 사용자를 지정합니다.

-user_dn_prefix *user_dn_prefix*
사용자를 작성할 때 사용할 구별 이름(DN) 접두어를 지정합니다.

-user_dn_suffix *user_dn_suffix*
사용자를 작성할 때 사용할 구별 이름(DN) 접미어를 지정합니다.

-verbose {true|false}
true로 설정할 경우 자세한 출력을 사용 가능하게 합니다. 기본값은 **false**입니다.

가용성

이 명령은 다음과 같은 기본 설치 디렉토리에 위치합니다.

- UNIX:

  `/opt/pdwls/sbin/`

- Windows 시스템의 경우:

  `C:\Program Files\Tivoli\pdwls\sbin\`

기본값 이외의 다른 설치 디렉토리를 선택할 때, 이 유틸리티는 설치 디렉토리 아래의 `sbin` 디렉토리(예: *`install_dir`*`\sbin\`)에 위치합니다.

리턴 코드

다음과 같은 종료 상태 코드가 리턴될 수 있습니다.

0 명령이 완료되었습니다.

1 명령에 실패했습니다.

명령에 실패하면 오류 메시지가 표시됩니다. 문제점의 자세한 설명에 대해서는 *IBM Tivoli Access Manager Error Message Reference*를 참조하십시오.

AMWLSConfigure -action delete_realm

WebLogic 서버에서 보안 범위를 삭제합니다.

구문

AMWLSConfigure -action delete_realm -domain_admin_pwd *domain_admin_pwd* **[-registry_clean {true|false}] [-verbose {true|false}]**

매개변수

-domain_admin_pwd *domain_admin_pwd*
WebLogic 도메인 관리자 암호를 지정합니다.

-registry_clean {true|false}
구성 중 작성된 사용자 및 그룹을 제거합니다. 기본값은 **false**입니다.

-verbose {true|false}
true로 설정할 경우 자세한 출력을 사용 가능하게 합니다. 기본값은 **false**입니다.

가용성

이 명령은 다음과 같은 기본 설치 디렉토리에 위치합니다.

- UNIX:

  /opt/pdwls/sbin/

- Windows 시스템의 경우:

  C:\Program Files\Tivoli\pdwls\sbin\

기본값 이외의 다른 설치 디렉토리를 선택할 때, 이 유틸리티는 설치 디렉토리 아래의 sbin 디렉토리(예: *install_dir*\sbin\)에 위치합니다.

리턴 코드

다음과 같은 종료 상태 코드가 리턴될 수 있습니다.

0 명령이 완료되었습니다.

1 명령에 실패했습니다.

명령에 실패하면 오류 메시지가 표시됩니다. 문제점의 자세한 설명에 대해서는 *IBM Tivoli Access Manager Error Message Reference*를 참조하십시오.

부록 C. 주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다. IBM은 다른 국가에서는 이 자료에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급하는 것이 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운용에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터
전화번호: 080-023-8080

2바이트(DBCS) 정보에 관한 라이센스 문의는 한국 IBM 고객만족센터에 문의하거나 다음 주소로 서면 문의하시기 바랍니다

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다. IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여 (단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증없이 이 책을 "현상태대로" 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및(또는) 프로그램을 사전 통지없이 언제든지 개선 및(또는) 변경할 수 있습니다.

© Copyright IBM Corp. 2003

이 정보에서 언급되는 비IBM의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(i) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (ii) 교환된 정보의 상호 이용을 목적으로 정보를 원하는 프로그램 라이센스 사용자는 다음 주소로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터

이러한 정보는 해당 조건(예를 들어, 사용료 지불 등)에 따라 사용할 수 있습니다.

이 정보에 기술된 라이센스가 부여된 프로그램 및 사용 가능한 모든 라이센스가 있는 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이센스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공된 것입니다.

본 문서에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 다른 운영 환경에서 얻어진 결과는 상당히 다를 수 있습니다. 일부 성능은 개발 레벨 상태의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한, 일부 성능은 추정을 통해 추측되었을 수도 있으므로 실제 결과는 다를 수 있습니다. 이 책의 사용자는 해당 데이터를 사용자의 특정 환경에서 검증해야 합니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 다른 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 비IBM 제품을 테스트하지 않았으므로, 이들 제품과 관련된 성능의 정확성, 호환성 또는 기타 주장에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM이 제시하는 방향 또는 의도에 관한 어떠한 언급도 특별한 통지없이 변경될 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이 예제에는 가능한 완벽하게 개념을 설명하기 위해 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

이 정보를 소프트카피로 보는 경우에는 사진과 컬러 삽화가 표시되지 않을 수도 있습니다.

상표

다음 용어는 미국 또는 기타 국가에서 사용되는 IBM Corporation의 상표 또는 등록 상표입니다.

AIX
DB2
IBM
IBM 로고
SecureWayTivoli
Tivoli 로고

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

Java 및 모든 Java 기반 등록 상표와 로고는 미국 또는 기타 국가에서 사용되는 Sun Microsystems,Inc의 상표 또는 등록 상표입니다.

UNIX는 미국 또는 기타 국가에서 사용되는 Open Group의 등록상표입니다.

기타 회사, 제품 및 서비스 이름은 타사의 상표 또는 서비스표입니다.

용어

가

가상 호스트(virtual hosting). 인터넷에 둘 이상의 호스트로 나타나도록 하는 웹 서버의 기능

개인용 키(private key). 컴퓨터 보안에서 소유자만이 사용할 수 있는 키. *공용 키*와 대조

공용 키(public key). 시스템 보안에서 모든 사람이 사용할 수 있는 키. *개인용 키*와 대조

관리 도메인(management domain). Tivoli Access Manager가 인증, 권한 부여 및 액세스 제어를 위해 보안 policy를 적용하는 기본 도메인. 이 도메인은 Policy Server가 구성될 때 작성됩니다. *도메인(domain)* 참조

관리 서버(management server). 더 이상 사용하지 않습니다. *Policy Server* 참조

관리 서비스(administration service). Tivoli Access Manager 자원 관리자 어플리케이션에서 관리 요청을 수행하기 위해 사용할 수 있는 권한 API 런타임 플러그인. 관리 서비스는 보호 오브젝트 트리 내의 특정 노드 아래에 오브젝트를 나열하는 것과 같이 태스크를 수행하기 위해 **pdadmin** 명령을 통해 원격 요청에 응답합니다. 고객은 권한 ADK를 사용하여 이러한 서비스를 개발할 수 있습니다.

구별 이름(DN: distinguished name). 디렉토리 내에서 항목을 식별하는 고유 이름. 구별 이름은 *속성:값* 쌍으로 구성되며, 쉼표로 구분합니다.

구성(configuration). (1) 정보 처리 시스템의 하드웨어 및 소프트웨어가 구성되어 상호 연결되는 방식. (2) 시스템, 서브시스템 또는 네트워크를 구성하는 시스템, 디바이스 및 프로그램

권한 룰(authorization rule). *룰(rule)* 참조

권한 서비스 플러그인(authorization service plug-in). 권한 API 내에서 서비스 인터페이스를 확장하는 작업을 수행하기 위해, 초기화 시 Tivoli Access Manager 권한 API 런타임 클라이언트에서 로드할 수 있는 동적으로 로드 가능한 라이브러리(DLL 또는 공유 라이브러리). 현재 사용 가능한 서비스 인터페이스에는 관리, 외부 권한, 권한 정보 수정, 인타이틀먼트 및 PAC 조작 인터페이스가 있습니다. 고객은 권한 ADK를 사용하여 이러한 서비스를 개발할 수 있습니다.

권한 정보 수정 서비스(credentials modification service). Tivoli Access Manager 권한 정보를 수정하기 위해 사용할 수 있는 권한 API 런타임 플러그인. 고객이 외부에서 개발한 권한 정보 수정 서비스는 권한 정보 속성 목록에 추가하고 이 목록에서 제거하는 조작을 수행하도록 제한되며, 수정 가능한 것으로 간주되는 속성들만으로 제한됩니다.

권한 정보(credentials). 인증 도중에 얻은 자세한 정보로, 사용자, 그룹 연관 및 기타 보안 관련 ID 속성에 대해 설명합니다. 권한 정보를 사용하여 다양한 서비스(예: 권한, 감사 및 위임)를 수행할 수 있습니다.

권한(authorization). (1) 시스템 보안에서 시스템과 통신하거나 시스템을 사용할 수 있도록 사용자에게 부여되는 권한. (2) 오브젝트, 자원 또는 기능에 대한 완전하거나 제한된 액세스를 사용자에게 부여하는 프로세스

권한(permission). 보호 오브젝트(예: 파일 또는 디렉토리)에 액세스할 수 있는 능력. 오브젝트에 해당하는 권한 수와 의미는 ACL(Access Control List)에서 정의됩니다. *ACL(Access Control List)* 참조

글로벌 사인 온(GSO: Global Signon). 사용자가 사용자 이름 및 암호를 백엔드 웹 어플리케이션 서버에 제공할 수 있도록 하는 융통성있는 싱글 사인 온 솔루션. 글로벌 사인 온은 단일 로그인을 통해 사용자가 사용할 권한이 있는 컴퓨팅 자원에 액세스할 수 있게 해 줍니다. 이기종의 분산 컴퓨팅 환경 내에서 여러 시스템 및 어플리케이션으로 구성된 큰 규모의 엔터프라이즈에 적합하게 만들어진 GSO를 사용하면 사용자는 여러 사용자 이름 및 암호를 관리하지 않아도 됩니다. *싱글 사인 온(SSO: Single Signon)* 참조

기본 인증(basic authentication). 보안 온라인 자원에 액세스할 수 있는 권한이 부여되기에 앞서, 사용자가 올바른 사용자 이름 및 암호를 입력해야 하는 인증 메소드

© Copyright IBM Corp. 2003

나

네트워크 기반 인증(network-based authentication). 사용자의 IP(Internet Protocol) 주소를 바탕으로 오브젝트 액세스를 제어하는 POP(Protected Object Policy). *POP(Protect Object Policy)* 참조

다

다중 요소 인증(multi-factor authentication). 사용자가 두 개 이상의 인증 레벨을 사용하여 인증하도록 강제 실행하는 POP(Protected Object Policy). 예를 들어, 보호 자원에 대한 액세스 제어에서 사용자는 사용자 이름/암호와 사용자 이름/토큰 암호 코드 둘다로 인증해야 합니다. *POP(Protected Object Policy)* 참조

단계별 인증(step-up authentication). 사전 구성된 인증 레벨 계층 구조에 의존하며, 자원의 policy 세트에 따라 특정 레벨의 인증을 강제 실행하는 POP(Protected Object Policy). 단계별 인증 POP를 사용하면 사용자가 주어진 자원에 액세스하기 위해 여러 레벨의 인증을 사용하지 않아도 되지만, 사용자가 최소한 자원을 보호하는 policy에서 요구하는 레벨에서 인증해야 합니다.

싱글 사인 온(SSO: Single Signon). 사용자가 한 번 로그온하면 각각의 어플리케이션에 개별적으로 로그온하지 않고도 여러 어플리케이션에 액세스할 수 있는 기능. *글로벌 사인 온(GSO: Global Signon)* 참조

도메인 이름(domain name). 인터넷 프로토콜군에서 호스트 시스템의 이름. 도메인 이름은 분리문자로 구분되는 일련의 하위 이름으로 구성됩니다. 예를 들어, 호스트 시스템의 완전한 도메인 이름(FQDN)이 as400.rchland.vnet.ibm.com일 경우, 다음은 각각 도메인 이름입니다. as400.rchland.vnet.ibm.com, vnet.ibm.com, ibm.com

도메인(domain). (1) 공통 서비스를 공유하며 보통 공통되는 목적으로 기능하는 사용자, 시스템 및 자원의 논리 그룹화. (2) 데이터 처리 자원이 공통 제어 하에 있는 시스템 네트워크 부분. *도메인 이름(domain name)* 참조

디렉토리 스키마(directory schema). 디렉토리에 나타날 수 있는 올바른 속성 유형 및 오브젝트 클래스. 속성 유형 및 오브젝트 클래스는 속성 값 구문(예를 들어, 어떤 속성이 존재해야 하는지, 그리고 디렉토리에 대해 어떤 속성이 존재할 수 있는지)을 정의합니다.

디먼(daemon). 연속 또는 주기적으로 시스템 범위의 기능(예: 네트워크 제어)을 수행하기 위해 무인으로 실행되는 프로그램. 일부 디먼은 해당 태스크를 수행하기 위해 자동으로 트리거되고, 나머지 디먼은 정기적으로 작동합니다.

디지털 서명(digital signature). e-commerce에서 데이터 단위에 추가되거나 데이터 단위의 암호 전송에 해당하는 데이터로, 데이터 단위 수신자가 단위의 무결성 및 소스를 확인하고 위조 가능성을 인식할 수 있게 합니다.

라

라우팅 파일(routing file). 메시지 구성을 제어하는 명령을 포함하는 ASCII 파일

런타임(run time). 시스템 프로그램을 실행하는 시간. 런타임 환경은 실행 환경입니다.

레지스트리(registry). 사용자, 시스템 및 소프트웨어에 대한 액세스 및 구성 정보를 포함하는 데이터 저장소

룰(rule). 이벤트 서버가 이벤트 간의 관계(이벤트 상관)를 인식하고 이에 따라 자동 응답을 실행할 수 있도록 하는 하나 이상의 논리 명령문

마

마이그레이션(migration). 이전 버전 또는 릴리스를 바꾸기 위해 프로그램의 새 버전 또는 릴리스를 설치하는 것

메타데이터(metadata). 저장된 데이터의 특성을 설명하는 데이터

바

바인드(bind). ID를 프로그램 내의 다른 오브젝트와 관련짓는 것. 예를 들어, ID를 값, 주소 또는 다른 ID와 관련짓거나, 형식적인 매개변수 및 실제 매개변수와 연관짓는 것

보안 관리(security management). 조직의 성공에 중요한 데이터 및 어플리케이션의 액세스를 제어하기 위한 조직의 능력을 지정하는 관리 규칙

보호 수준(quality of protection). 인증, 무결성 및 프라이버시 조건 조합으로 판별되는 데이터 보안 수준

보호 오브젝트 공간(protected object space). ACL 및 POP를 적용하기 위해 사용하며 사용자 액세스 권한 부여에 사용하

는 실제 시스템 자원의 가상 오브젝트 표시. *보호 오브젝트 (protected object)* 및 *POP(Protect Object Policy)* 참조

보호 오브젝트(protected object). ACL 및 POP를 적용하기 위해 사용하며 사용자 액세스 권한 부여에 사용하는 실제 시스템 자원의 논리 표시. *POP(Protect Object Policy)* 및 *보호 오브젝트 공간(protected object space)* 참조

복제본(replica). 다른 서버의 디렉토리 사본을 포함하는 서버. 복제본은 성능 또는 응답 시간을 향상시키고 데이터 무결성을 보장하기 위해 서버를 백업합니다.

블레이드(blade). 어플리케이션 특정 서비스 및 구성요소를 제공하는 구성요소

비즈니스 인타이틀먼트(business entitlement). 자원에 관한 권한 요청에서 사용할 수 있는 자세한 조건을 설명하는 사용자 권한 정보의 보충 속성

사

사용자 레지스트리(user registry). *레지스트리(registry)* 참조

사용자(user). 다른 개인, 조직, 프로세스, 디바이스, 프로그램, 프로토콜 또는 시스템에서 제공하는 서비스를 사용하는 모든 개인, 조직, 프로세스, 디바이스, 프로그램, 프로토콜 또는 시스템

서비스(service). 서버에서 수행되는 작업. 서비스는 데이터를 보내거나 저장하기 위한 단순한 요청이거나(파일 서버, HTTP Server, 전자 우편 서버 및 핑거 서버에서), 더 복잡한 작업(예: 인쇄 서버 또는 프로세스 서버의 서비스)일 수 있습니다.

속성 목록(attribute list). 권한을 결정하기 위해 사용하는 확장 정보를 포함하는 링크된 목록. 속성 목록은 *이름 = 값* 쌍으로 구성됩니다.

스키마(schema). 데이터베이스 구조를 완전하게 설명하는 명령문 세트로, 데이터 정의 언어로 표현됩니다. 관계형 데이터베이스에서 스키마는 테이블, 각 테이블의 필드, 필드와 테이블 간의 관계를 정의합니다.

신뢰성있는 루트(trusted root). SSL(Secure Sockets Layer)에서 CA(Certificate Authority)의 공용 키 및 연관된 구별 이름

아

암호화(encryption). 시스템 보안에서 원래 데이터를 암호 해독 프로세스만을 사용하여 볼 수 있도록 난해한 형태로 변환하는 프로세스

암호(cipher). 키를 사용하여 보통 데이터로 변환(암호 해독)되기 전에는 읽을 수 없도록 암호화된 데이터

액세스 권한(access permission). 전체 오브젝트에 적용하는 액세스 권한

액세스 제어(access control). 시스템 보안에서 권한이 있는 사용자만이 권한이 부여된 방식으로 시스템 자원에 액세스할 수 있도록 보장하는 프로세스.

역할 지정(role assignment). 사용자가 해당 역할에 정의된 오브젝트에 관해 적절한 액세스 권한을 갖는 것처럼, 사용자에게 역할을 지정하는 프로세스

역할 활성화(role activation). 역할에 액세스 권한을 적용하는 프로세스

연결(connection). (1) 데이터 통신에서 정보 전달을 위한 기능 장치 사이에 설정되는 연관. (2) TCP/IP에서 신뢰할 수 있는 데이터 스트림 전달 서비스를 제공하는 두 개의 프로토콜 어플리케이션 사이의 경로. 인터넷에서 연결은 한 시스템의 TCP 어플리케이션에서 다른 시스템의 TCP 어플리케이션으로 확장합니다. (3) 시스템 통신에서 두 시스템 사이 또는 시스템과 디바이스 사이에 데이터를 전달할 수 있는 회선

외부 권한 서비스(external authorization service). Tivoli Access Manager 권한 결정 체인의 일부로 어플리케이션 또는 환경 특정 권한 결정을 위해 사용할 수 있는 권한 API 런타임 플러그인. 고객은 권한 ADK를 사용하여 이러한 서비스를 개발할 수 있습니다.

응답 파일(response file). 프로그램에서 요청하는 질문에 맞는 사전정의된 응답 세트를 포함하며, 한 번에 하나씩 값을 입력하는 대신 사용되는 파일

인증서(certificate). 시스템 보안에서 공용 키를 인증서 소유자의 ID에 바인드하여 인증서 소유자를 인증할 수 있도록 하는 디지털 문서. 인증서는 CA(Certificate Authority)에서 발급합니다.

인증(authentication). (1) 시스템 보안에서 사용자 ID 또는 사용자의 오브젝트 액세스 권한을 확인하는 것. (2) 시스템 보안에서 메시지가 변경 또는 손상되지 않았는지 확인하는 것. (3) 시스템 보안에서 정보 시스템 또는 보호 자원의 사용자를 확인하

기 위해 사용하는 프로세스. *다중 요소 인증*, *네트워크 기반 인증(authentication)* 및 *단계별 인증(authentication)* 참조

인타이틀먼트 서비스(entitlement service). 프린시펄 또는 조건 세트의 외부 소스로부터 인타이틀먼트를 리턴하기 위해 사용할 수 있는 권한 API 런타임 플러그인. 인타이틀먼트는 보통 특정 방식으로 자원 관리자 어플리케이션에서 소비하거나 나중에 권한 프로세스에서 사용하기 위해 프린시펄의 권한 정보에 추가할 어플리케이션 특정 데이터입니다. 고객은 권한 ADK를 사용하여 이러한 서비스를 개발할 수 있습니다.

인타이틀먼트(entitlement). 외부화된 보안 policy 정보를 포함하는 데이터 구조. 권한에는 특정 어플리케이션으로 이해할 수 있는 방식으로 형식화된 기능 또는 policy 데이터가 있습니다.

인터넷 프로토콜군(Internet suite of protocols). 인터넷에서 사용하기 위해 개발되어 IETF(Internet Engineering Task Force)를 통해 RFC(Requests for Comment)로 공개된 프로토콜 세트

자

자동 설치(silent installation). 메시지를 콘솔에 보내지 않지만 대신 로그 파일에 메시지와 오류를 저장하는 설치. 또한 자동 설치에서는 데이터 입력을 위해 응답 파일을 사용할 수 있습니다. *응답 파일(response file)* 참조

자원 오브젝트(resource object). 실제 네트워크 자원(예: 서비스, 파일 및 프로그램)의 표시

자체 등록(self-registration). 사용자가 필요한 데이터를 입력할 수 있고 관리자의 관여 없이 등록된 Tivoli Access Manager 사용자가 될 수 있는 프로세스

접미어(suffix). 로컬로 보유하는 디렉토리 계층 구조에서 맨 위 항목을 식별하는 구별 이름. LDAP(Lightweight Directory Access Protocol)에서 사용되는 상대적 이름지정 방식으로 인해, 이 접미어는 디렉토리 계층 구조 내의 다른 모든 항목에 적용됩니다. 디렉토리 서버에는 로컬로 보유되는 디렉토리 계층 구조 각각을 식별하는 여러 개의 접미어가 있을 수 있습니다.

조치(action). ACL(Access Control List) 권한 속성. *ACL(Access Control List)* 참조

카

컨테이너 오브젝트(container object). 오브젝트 공간을 별도의 기능 region에 구성하는 구조적 지정

쿠키(cookie). 서버가 클라이언트 시스템에 저장하고 후속 세션에서 액세스하는 정보. 쿠키는 서버가 클라이언트에 대한 특정 정보를 기억할 수 있게 합니다.

크기 조정 가능(scalability). 자원에 액세스하는 사용자 수의 증가에 응답하기 위한 네트워크 시스템 기능

키 데이터베이스 파일(key database file). *키 링(key ring)* 참조

키 링(key ring). 시스템 보안에서 공용 키, 개인용 키, 신뢰성 있는 루트 및 인증을 포함하는 파일

키 쌍(key pair). 시스템 보안에서 공용 키 및 개인용 키. 암호화에 키 쌍을 사용할 때, 송신자는 공용 키를 사용하여 메시지를 암호화하고, 수신자는 개인용 키를 사용하여 메시지를 암호 해독합니다. 서명에 키 쌍을 사용할 때, 서명자는 개인용 키를 사용하여 메시지 표시를 암호화하고, 수신자는 공용 키를 사용하여 서명 확인을 위해 메시지 표시를 암호 해독합니다.

키 파일(key file). *키 링(key ring)* 참조

키(key). 시스템 보안에서 데이터 암호화 및 암호 해독을 위해 암호화 알고리즘에서 사용하는 일련의 기호. *개인용 키(private key)* 및 *공용 키(public key)* 참조

타

토큰(token). (1) 근거리 통신망에서 스테이션이 임시로 전송 매체 제어 하에 있음을 표시하기 위해 데이터 스테이션 간에 연속적으로 전달되는 권한 기호. 각각의 데이터 스테이션에는 매체를 제어하기 위해 토큰을 획득하고 사용할 기회가 있습니다. 토큰은 전송 권한을 알리는 특정 메시지 또는 비트 패턴입니다. (2) 근거리 통신망(LAN)에서 전송 매체와 함께 디바이스 간에 전달되는 비트 시퀀스. 토큰에 데이터가 추가된 경우, 이 토큰은 프레임이 됩니다.

파

포털(portal). 특정 사용자의 액세스 권한을 기반으로, 특정 사용자가 사용 가능한 웹 자원(예: 링크, 내용 또는 서비스)의 사용자 정의 목록을 동적으로 작성하는 통합 웹 사이트

폴링(polling). 데이터의 전송 여부를 결정하기 위해 데이터베이스를 정기적으로 조사하는 프로세스

하

호스트(host). 네트워크(예: 인터넷 또는 SNA 네트워크)에 연결되어 있고 그 네트워크에 액세스하는 지점을 제공하는 시스템. 또한 호스트는 환경에 따라 네트워크의 중앙 집중화된 제어를 제공할 수도 있습니다. 호스트는 클라이언트 서버, 또는 동시에 클라이언트와 서버 둘다가 될 수 있습니다.

A

ACL. *ACL(Access Control List)* 참조

ACL(Access Control List). 시스템 보안에서 오브젝트에 액세스할 수 있는 모든 주체와 해당 액세스 권한을 식별하는 오브젝트와 연관되는 목록. 예를 들어, ACL은 파일에 액세스할 수 있는 사용자를 식별하고 이 파일에 대해 사용자가 가지고 있는 액세스 권한을 식별하는 파일과 연관된 목록입니다.

B

BA. *기본 인증(basic authentication)* 참조

C

CA. *CA(Certificate Authority)* 참조

CA(Certificate Authority). 인증서를 발급하는 기관. CA(Certificate Authority)는 인증서 소유자의 ID와 그 소유자에게 사용 권한이 부여된 서비스 인증, 새 인증서 발급, 기존 인증서 재발급, 사용할 권한이 더 이상 없는 사용자의 인증서 폐기 등을 수행합니다.

CDAS. *CDAS(Cross Domain Authentication Service)* 참조

CDAS(Cross Domain Authentication Service). 기본 WebSEAL 인증 메커니즘을, Tivoli Access Manager ID를 WebSEAL에 리턴하는 사용자 정의 프로세스로 대체 가능하게 하는 공유 라이브러리 메커니즘을 제공하는 WebSEAL 서비스. *WebSEAL* 참조

CDMF. *CDMF(Cross Domain Mapping Framework)* 참조

CDMF(Cross Domain Mapping Framework). 개발자가 WebSEA e-Community SSO 기능을 사용할 때 사용자 ID 맵핑 및 사용자 속성 처리를 사용자에 맞게 정의할 수 있게 하는 프로그래밍 인터페이스

CGI. *CGI(Common Cateway Interface)* 참조

CGI(Common Cateway Interface). HTTP 요청을 통해 웹 서버에서 어플리케이션으로 정보를 전달하는 스크립트를 정의하기 위한 인터넷 표준. 반대의 경우도 마찬가지입니다. CGI 스크립트는 스크립트 언어(예: Perl)로 작성된 CGI 프로그램입니다.

D

DN. *구별 이름(distinguished name:DN)* 참조

E

EAS. *외부 권한 서비스(External Authorization Service)* 참조

F

FTP(File Transfer Protocol). 인터넷 프로토콜군에서 시스템이나 호스트 사이에 대량 데이터 파일을 전송하기 위해 TCP 및 Telnet 서비스를 사용하는 어플리케이션 계층 프로토콜

G

GSO. *GSO(Global Signon)* 참조

H

HTTP. *HTTP(Hypertext Transfer Protocol)* 참조

HTTP(Hypertext Transfer Protocol). 인터넷 프로토콜군에서 하이퍼텍스트 문서를 전송하고 표시하기 위해 사용하는 프로토콜

I

IP. *IP(Internet Protocol)* 참조

IPC. *IPC(Interprocess Communication)* 참조

IPC(Interprocess Communication). (1) 프로그램이 서로 데이터를 송수신하고 활동을 동기화하는 프로세스 세마포어, 신호 및 내부 메시지 큐가 프로세스 간 통신의 공통 방법입니다. (2) 프로세스가 동일한 시스템 내 또는 네트워크를 통해 다른 프로세스와 서로 통신할 수 있도록 하는 운영 체제 메커니즘

IP(Internet Protocol). 인터넷 프로토콜군에서 데이터를 네트워크 또는 상호 연결된 네트워크를 통해 라우트하고 상위 프로토콜 계층과 실제 네트워크 사이의 중계 역할을 하는 연결 없는 프로토콜

J

junction. 프론트엔드 WebSEAL 서버와 백엔드 웹 어플리케이션 서버 간의 HTTP 또는 HTTPS 연결. WebSEAL은 junction을 사용하여 백엔드 서버 대신 보호 서비스를 제공하게 합니다.

L

LDAP. *LDAP(Lightweight Directory Access Protocol)* 참조

LDAP(Lightweight Directory Access Protocol). (a) X.500 모델을 지원하는 디렉토리에 액세스할 수 있는 권한을 제공하기 위해 TCP/IP를 사용하고, (b) 더 복잡한 X.500 DAP(Directory Access Protocol)의 자원 요구사항을 만족하는 개방 프로토콜. LDAP를 사용하는 어플리케이션(디렉토리 사용 가능 어플리케이션이라고도 함)은 개인 또는 서비스에 대한 정보(예: 전자 우편 주소, 공용 키 또는 서비스 특정 구성 매개변수) 검색을 위해 공통 데이터 저장소로 디렉토리를 사용할 수 있습니다. LDAP는 원래 RFC 1777에 지정되어 있었습니다. LDAP 버전 3은 RFC 2251에 지정되어 있으며, IETF는 계속해서 추가 표준 기능에 대해 연구하고 있습니다. IETF에서 정의한 일부 LDAP용 표준 스키마는 RFC 2256에서 볼 수 있습니다.

LTPA. *LTPA(Lightweight Third Party Authentication)* 참조

LTPA(Lightweight Third Party Authentication). 인터넷 도메인 내에 속해 있는 웹 서버 세트를 거쳐 싱글 사인 온을 허용하는 인증 프레임워크

M

MPA(Multiplexing Proxy Agent). 여러 클라이언트 액세스를 조절하는 게이트웨이. 이 게이트웨이는 간혹 클라이언트가 WAP를 사용하여 보안 도메인에 액세스할 경우, WAP(Wireless Access Protocol) 게이트웨이라고도 합니다. 게이트웨이는 원래 서버에 단일 인증된 채널을 설정하고, 모든 클라이언트 요청 및 응답을 이 채널을 통해 터널링합니다.

P

PAC. *PAC(Privilege Attribute Certificate)* 참조.

PAC 서비스(privilege attribute certificate service). 사전에 판별된 형식의 PAC를 Tivoli Access Manager 권한 정보로, 또는 그 반대로 변환하는 권한 API 런타임 클라이언트 플러그인. 이러한 서비스는 보안 도메인의 다른 구성원에게 전송하기 위해 Tivoli Access Manager 권한 정보를 패키징하거나 정렬할 경우에도 사용할 수 있습니다. 고객은 권한 ADK를 사용하여 이러한 서비스를 개발할 수 있습니다. *PAC(Privilege Attribute Certificate)* 참조

PAC(Privilege Attribute Certificate). 프린시펄(사용자)의 인증과 권한 부여 속성 및 프린시펄(사용자)의 기능을 포함하는 디지털 문서

policy. 관리 자원에 적용되는 룰 세트

Policy Server. 보안 도메인에서 다른 서버에 대한 위치 정보를 유지보수하는 Tivoli Access Manager 서버

POP. *POP(Protect Object Policy)* 참조

POP(Protect Object Policy). 보호 오브젝트에 액세스할 수 있도록 ACL policy가 허용하는 조작에 추가 조건을 적용하는 보안 policy 유형. POP 조건을 적용하는 것은 자원 관리자의 책임입니다. *ACL(Access Control List), 보호 오브젝트(protected object)* 및 *보호 오브젝트 공간(protected object space)* 참조

R

RSA 암호화 시스템(RSA encryption). 암호화 및 인증에 사용하는 공용 키 암호화 시스템. 1977년 Ron Rivest, Adi Shamir 및 Leonard Adleman에 의해 고안된 암호화 시스템입니다. 두 개의 큰 소수값 곱을 인수분해하는 어려움의 정도에 따라, 시스템 보안이 달라집니다.

S

SSL. *SSL(Secure Sockets Layer)* 참조

SSL(Secure Sockets Layer). 통신 프라이버시를 제공하는 보안 프로토콜. SSL은 클라이언트/서버 어플리케이션이 도청, 간섭 및 메시지 위조를 방지하기 위해 만들어진 방식으로 통신할 수 있게 합니다. SSL은 Netscape Communications Corp.와 RSA Data Security, Inc.에서 개발했습니다.

SSO. *SSO(Single Signon)* 참조

U

URI. *URI(Uniform Resource Identifier)* 참조

URI(Uniform Resource Identifier). 자원 이름(디렉토리 및 파일 이름), 자원 위치(디렉토리 및 파일 이름이 있는 시스템) 및 자원 액세스 방법 프로토콜(예: HTTP)을 포함하여 인터넷의 컨

텐츠를 식별하기 위해 사용되는 문자열. URI의 한 예로는 고유한 자원 위치 지정자, 즉 URL이 있습니다.

URL. *URL(Uniform Resource Locator)* 참조

URL(Uniform Resource Locator). 시스템 또는 인터넷과 같은 네트워크(예: 인터넷)에서 정보 자원을 표시하는 문자 시퀀스. 이 문자 시퀀스에는 (a) 정보 자원에 액세스하기 위해 사용하는 프로토콜의 축약된 이름과 (b) 정보 자원을 찾기 위해 프로토콜에서 사용하는 정보가 있습니다. 예를 들어, 인터넷 컨텍스트에서 이들은 다양한 정보 자원에 액세스하기 위해 사용하는 프로토콜의 축약된 이름입니다(예: http, ftp, gopher, telnet 및 news). IBM 홈 페이지의 URL은 http://www.ibm.com입니다.

W

WebSEAL. Tivoli Access Manager 블레이드. WebSEAL은 보호 오브젝트 공간에 보안 policy를 적용하는 고성능의 다중 스레드 웹 서버입니다. WebSEAL은 싱글 사인 온 솔루션을 제공하고 백엔드 웹 어플리케이션 서버 자원을 보안 policy에 통합할 수 있습니다.

WPM. *WPM(Web Portal Manager)* 참조

WPM(Web Portal Manager). 보안 도메인에서 Tivoli Access Manager 기본 및 WebSEAL 보안 policy를 관리하기 위해 사용하는 웹 기반 그래픽 어플리케이션. **pdadmin** 명령행 인터페이스에 대한 대안으로, 이 GUI는 원격 관리자 액세스를 가능하게 하고, 관리자가 위임된 사용자 도메인을 작성하여 이 도메인에 위임 관리자를 지정할 수 있게 합니다.

색인

[가]

관련 서적 xi
구성된 사용자 7, 43
권한
  선언 41
  프로그램 41
기본 인증
  구성된 사용자 7

[다]

데모 어플리케이션 41
디스크 요구사항 11

[라]

로그온 policy 44

[마]

메모리 요구사항 11
문제점 판별 46
문제점 해결
  메모리 부족 문제점 47
  인증 46

[사]

사용 팁 43
사전 설치 소프트웨어
  소프트웨어 12
선언 권한 41
설치 17
  AIX 17
  HP-UX 18
  Solaris 19
  Windows 20
싱글 사인 온 13
  데모 어플리케이션으로 테스트 43

[아]

언어 팩
  비영어 25
유틸리티
  AMWLSConfigure -action config 64
  AMWLSConfigure -action create_realm 67
  AMWLSConfigure -action delete realm 69
  AMWLSConfigure -action unconfig 66
인증
  외부 사용자 6
  Access Manager 6
  WebSEAL 사용 6
  WebSEAL 없음 7

[자]

작성
  WebSEAL junction
    pdadmin 사용 32
제거 지시사항
  AIX 50
  HP-UX 51
  Solaris 49
  Windows 50
제한사항
  그룹 내의 그룹 47
  J2EE 자원 관리 47
  java.security.ACL 인터페이스 47
지원 플랫폼 11

[파]

프로그램 권한 41

A

Access Manager
  보안 모델 1
  Java Runtime Environment 23
  Java 런타임 환경 14
  pdjrtecfg 23
  Policy Server 12
  WebSEAL 13

© Copyright IBM Corp. 2003

AIX
  설치 17
  제거 50
AMWLSConfigure -action config 64
AMWLSConfigure -action create_realm 67
AMWLSConfigure -action delete realm 69
AMWLSConfigure -action unconfig 66

C

CLASSPATH
  언어 팩으로 startWebLogic 설정 25
  startWebLogic 설정 25

H

HP-UX
  설치 18
  제거 51

I

installp 17

J

Java
  AIX의 런타임 13
junctions
  구성 32

P

pdadmin
  WebSEAL junction 작성 32
pdjrtecfg
  명령행 23
pkgadd 19
pkgrm 49
policy
  로그온 44
Policy Server 12

S

SMIT 50
Solaris
  설치 19
Solaris *(계속)*
  제거 49
startWebLogic
  명령 위치 25
startWebLogic, CLASSPATH 설정 25
swinstall 18
swremove 51

T

Tivoli Access Manager for WebLogic 제거
  방법 49

W

WebLogic 서버
  버전 7.0 지원 11
  서비스 팩 11
  호환 모드 11
  Security Service Provider Interface 11
WebSEAL 2, 13
  구성된 사용자 7
  싱글 사인 온 13, 32
  인증 6
WebSEAL junctions
  구성 32
Windows
  설치 20
  제거 50

Printed in Denmark by IBM Danmark A/S

SA30-2210-00